List of built-in policy definitions - Azure Policy

By rmcmurray

Archived: 2026-04-06 00:33:15 UTC

[Preview]: Configure subscriptions to enable service health alert monitoring rule Assignable at the subscription or management group level, this policy ensures that each subscription has a service health alert rule configured with alert conditions and mapping to action groups as specified in the policy parameters. By default creates a resource group, alert rule and action group configured to send emails to subscription owners for all service health events. DeployIfNotExists, AuditIfNotExists, Disabled 1.3.0-preview [Preview]: Configure system-assigned managed identity to enable Azure Monitor assignments on VMs Configure system-assigned managed identity to virtual machines hosted in Azure that are supported by Azure Monitor and do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Azure Monitor assignments and must be added to machines before using any Azure Monitor extension. Target virtual machines must be in a supported location. Modify, Disabled 6.2.0-preview [Preview]: Data Collection Rules that target a specific workspace should use the specified Data Collection Endpoint Audit or deny the creation of DCRs that target a workspace and don't use the specified DCE Audit, Deny, Disabled 1.0.0-preview [Preview]: Network traffic data collection agent should be installed on Linux virtual machines Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats. AuditIfNotExists, Disabled 1.0.2-preview [Preview]: Network traffic data collection agent should be installed on Windows virtual machines Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats. AuditIfNotExists, Disabled 1.0.2-preview Activity log should be retained for at least one year This policy audits the activity log if the retention is not set for 365 days or forever (retention days set to 0). AuditIfNotExists, Disabled 1.0.0 An activity log alert should exist for specific Administrative operations This policy audits specific Administrative operations with no activity log alerts configured. AuditIfNotExists, Disabled 1.0.0 An activity log alert should exist for specific Policy operations This policy audits specific Policy operations with no activity log alerts configured. AuditIfNotExists, Disabled 3.0.0 An activity log alert should exist for specific Security operations This policy audits specific Security operations with no activity log alerts configured. AuditIfNotExists, Disabled 1.1.0 Application Insights components should block log ingestion and querying from public networks Improve Application Insights security by blocking log ingestion and querying from public networks. Only private-link connected networks will be able to ingest and query logs of this component. Learn more at https://aka.ms/AzMonPrivateLink#configure-application-insights. audit, Audit, deny, Deny, disabled, Disabled 1.1.0 Application Insights components should block non-Azure Active Directory based ingestion. Enforcing log ingestion to require Azure Active Directory authentication prevents unauthenticated logs from an attacker which could lead to incorrect status, false alerts, and incorrect logs stored in the system. Deny, Audit, Disabled 1.0.0 Application Insights components with Private Link enabled should use Bring Your Own Storage accounts for profiler and debugger. To support private link and customer-managed key policies, create your own storage

account for profiler and debugger. Learn more in https://docs.microsoft.com/azure/azure-monitor/app/profiler-bring-your-own-storage Deny, Audit, Disabled 1.0.0 Audit diagnostic setting for selected resource types Audit diagnostic setting for selected resource types. Be sure to select only resource types which support diagnostics settings. AuditIfNotExists 2.0.1 Azure Application Gateway should have Resource logs enabled Enable Resource logs for Azure Application Gateway (plus WAF) and stream to a Log Analytics workspace. Get detailed visibility into inbound web traffic and actions taken to mitigate attacks. AuditIfNotExists, Disabled 1.0.0 Azure Front Door should have Resource logs enabled Enable Resource logs for Azure Front Door (plus WAF) and stream to a Log Analytics workspace. Get detailed visibility into inbound web traffic and actions taken to mitigate attacks. AuditIfNotExists, Disabled 1.0.0 Azure Front Door Standard or Premium (Plus WAF) should have resource logs enabled Enable Resource logs for Azure Front Door Standard or Premium (plus WAF) and stream to a Log Analytics workspace. Get detailed visibility into inbound web traffic and actions taken to mitigate attacks. AuditIfNotExists, Disabled 1.0.0 Azure Log Search Alerts over Log Analytics workspaces should use customer-managed keys Ensure that Azure Log Search Alerts are implementing customer-managed keys, by storing the query text using the storage account that the customer had provided for the queried Log Analytics workspace. For more information, visit https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview. Audit, Disabled, Deny 1.0.0 Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action' This policy ensures that a log profile collects logs for categories 'write,' 'delete,' and 'action' AuditIfNotExists, Disabled 1.0.0 Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption) To ensure secure data encryption is enabled at the service level and the infrastructure level with two different encryption algorithms and two different keys, use an Azure Monitor dedicated cluster. This option is enabled by default when supported at the region, see https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview. audit, Audit, deny, Deny, disabled, Disabled 1.1.0 Azure Monitor Logs clusters should be encrypted with customer-managed key Create Azure Monitor logs cluster with customer-managed keys encryption. By default, the log data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance. Customer-managed key in Azure Monitor gives you more control over the access to you data, see https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys. audit, Audit, deny, Deny, disabled, Disabled 1.1.0 Azure Monitor Logs for Application Insights should be linked to a Log Analytics workspace Link the Application Insights component to a Log Analytics workspace for logs encryption. Customer-managed keys are commonly required to meet regulatory compliance and for more control over the access to your data in Azure Monitor. Linking your component to a Log Analytics workspace that's enabled with a customer-managed key, ensures that your Application Insights logs meet this compliance requirement, see https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys. audit, Audit, deny, Deny, disabled, Disabled 1.1.0 Azure Monitor Private Link Scope should block access to non private link resources Azure Private Link lets you connect your virtual networks to Azure resources through a private endpoint to an Azure Monitor Private Link scope (AMPLS). Private Link Access modes are set on your AMPLS to control whether ingestion and query requests from your networks can reach all resources, or only Private Link resources (to prevent data exfiltration). Learn more about private links at: https://docs.microsoft.com/azure/azure-monitor/logs/private-link-security#private-link-access-modes-private-only-vs-open. Audit, Deny, Disabled 1.0.0 Azure Monitor Private Link Scope should use private link Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping

private endpoints to Azure Monitor Private Links Scope, you can reduce data leakage risks. Learn more about private links at: https://docs.microsoft.com/azure/azure-monitor/logs/private-link-security. AuditIfNotExists, Disabled 1.0.0 Azure Monitor should collect activity logs from all regions This policy audits the Azure Monitor log profile which does not export activities from all Azure supported regions including global. AuditIfNotExists, Disabled 2.0.0 Azure Monitor solution 'Security and Audit' must be deployed This policy ensures that Security and Audit is deployed. AuditIfNotExists, Disabled 1.0.0 Azure subscriptions should have a log profile for Activity Log This policy ensures if a log profile is enabled for exporting activity logs. It audits if there is no log profile created to export the logs either to a storage account or to an event hub. AuditIfNotExists, Disabled 1.0.0 Configure Azure Activity logs to stream to specified Log Analytics workspace Deploys the diagnostic settings for Azure Activity to stream subscriptions audit logs to a Log Analytics workspace to monitor subscription-level events DeployIfNotExists, Disabled 1.0.0 Configure Azure Application Insights components to disable public network access for log ingestion and querying Disable components log ingestion and querying from public networks access to improve security. Only private-link connected networks will be able to ingest and query logs on this workspace. Learn more at https://aka.ms/AzMonPrivateLink#configure-application-insights. Modify, Disabled 1.1.0 Configure Azure Log Analytics workspaces to disable public network access for log ingestion and querying Improve workspace security by blocking log ingestion and querying from public networks. Only private-link connected networks will be able to ingest and query logs on this workspace. Learn more at https://aka.ms/AzMonPrivateLink#configure-log-analytics. Modify, Disabled 1.1.0 Configure Azure Monitor Private Link Scope to block access to non private link resources Azure Private Link lets you connect your virtual networks to Azure resources through a private endpoint to an Azure Monitor Private Link scope (AMPLS). Private Link Access modes are set on your AMPLS to control whether ingestion and query requests from your networks can reach all resources, or only Private Link resources (to prevent data exfiltration). Learn more about private links at: https://docs.microsoft.com/azure/azure-monitor/logs/private-link-security#private-link-access-modes-private-only-vs-open. Modify, Disabled 1.0.0 Configure Azure Monitor Private Link Scope to use private DNS zones Use private DNS zones to override the DNS resolution for a private endpoint. A private DNS zone links to your virtual network to resolve to Azure Monitor private link scope. Learn more at: https://docs.microsoft.com/azure/azure-monitor/logs/private-link-security#connect-to-a-private-endpoint. DeployIfNotExists, Disabled 1.0.0 Configure Azure Monitor Private Link Scopes with private endpoints Private endpoints connect your virtual networks to Azure services without a public IP address at the source or destination. By mapping private endpoints to Azure Monitor Private Link Scopes, you can reduce data leakage risks. Learn more about private links at: https://docs.microsoft.com/azure/azure-monitor/logs/private-link-security. DeployIfNotExists, Disabled 1.0.0 Configure Dependency agent on Azure Arc enabled Linux servers Enable VM insights on servers and machines connected to Azure through Arc enabled servers by installing the Dependency agent virtual machine extension. VM insights uses the Dependency agent to collect network metrics and discovered data about processes running on the machine and external process dependencies. See more - https://aka.ms/vminsightsdocs. DeployIfNotExists, Disabled 2.1.0 Configure Dependency agent on Azure Arc enabled Linux servers with Azure Monitoring Agent settings Enable VM insights on servers and machines connected to Azure through Arc enabled servers by installing the Dependency agent virtual machine extension with Azure Monitoring Agent settings. VM insights uses the Dependency agent to collect network metrics and discovered data about processes running on the machine and external process dependencies. See more - https://aka.ms/vminsightsdocs. DeployIfNotExists, Disabled 1.2.0 Configure Dependency agent on Azure Arc enabled Windows servers Enable VM insights on servers and machines connected to Azure through Arc enabled

servers by installing the Dependency agent virtual machine extension. VM insights uses the Dependency agent to collect network metrics and discovered data about processes running on the machine and external process dependencies. See more - https://aka.ms/vminsightsdocs. DeployIfNotExists, Disabled 2.1.0 Configure Dependency agent on Azure Arc enabled Windows servers with Azure Monitoring Agent settings Enable VM insights on servers and machines connected to Azure through Arc enabled servers by installing the Dependency agent virtual machine extension with Azure Monitoring Agent settings. VM insights uses the Dependency agent to collect network metrics and discovered data about processes running on the machine and external process dependencies. See more - https://aka.ms/vminsightsdocs. DeployIfNotExists, Disabled 1.2.0 Configure Linux Arc Machines to be associated with a Data Collection Rule or a Data Collection Endpoint Deploy Association to link Linux Arc machines to the specified Data Collection Rule or the specified Data Collection Endpoint. The list of locations are updated over time as support is increased. DeployIfNotExists, Disabled 2.2.1 Configure Linux Arc-enabled machines to run Azure Monitor Agent Automate the deployment of Azure Monitor Agent extension on your Linux Arc-enabled machines for collecting telemetry data from the guest OS. This policy will install the extension if the region is supported. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 2.4.0 Configure Linux Machines to be associated with a Data Collection Rule or a Data Collection Endpoint Deploy Association to link Linux virtual machines, virtual machine scale sets, and Arc machines to the specified Data Collection Rule or the specified Data Collection Endpoint. The list of locations and OS images are updated over time as support is increased. DeployIfNotExists, Disabled 6.8.0 Configure Linux Virtual Machine Scale Sets to be associated with a Data Collection Rule or a Data Collection Endpoint Deploy Association to link Linux virtual machine scale sets to the specified Data Collection Rule or the specified Data Collection Endpoint. The list of locations and OS images are updated over time as support is increased. DeployIfNotExists, Disabled 4.7.0 Configure Linux virtual machine scale sets to run Azure Monitor Agent with system-assigned managed identity-based authentication Automate the deployment of Azure Monitor Agent extension on your Linux virtual machine scale sets for collecting telemetry data from the guest OS. This policy will install the extension if the OS and region are supported and system-assigned managed identity is enabled, and skip install otherwise. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 3.10.0 Configure Linux virtual machine scale sets to run Azure Monitor Agent with user-assigned managed identity-based authentication Automate the deployment of Azure Monitor Agent extension on your Linux virtual machine scale sets for collecting telemetry data from the guest OS. This policy will install the extension and configure it to use the specified user-assigned managed identity if the OS and region are supported, and skip install otherwise. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 3.11.0 Configure Linux Virtual Machines to be associated with a Data Collection Rule or a Data Collection Endpoint Deploy Association to link Linux virtual machines to the specified Data Collection Rule or the specified Data Collection Endpoint. The list of locations and OS images are updated over time as support is increased. DeployIfNotExists, Disabled 4.7.0 Configure Linux virtual machines to run Azure Monitor Agent with system-assigned managed identity-based authentication Automate the deployment of Azure Monitor Agent extension on your Linux virtual machines for collecting telemetry data from the guest OS. This policy will install the extension if the OS and region are supported and system-assigned managed identity is enabled, and skip install otherwise. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 3.10.0 Configure Linux virtual machines to run Azure Monitor Agent with user-assigned managed identity-based authentication Automate the deployment of Azure Monitor Agent extension on your Linux virtual machines for collecting telemetry data from the guest OS. This policy will install the extension and configure it to use the specified user-assigned managed identity if the OS and region are supported, and skip install otherwise. Learn

more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 3.14.0 Configure Log Analytics workspace and automation account to centralize logs and monitoring Deploy resource group containing Log Analytics workspace and linked automation account to centralize logs and monitoring. The automation account is aprerequisite for solutions like Updates and Change Tracking. DeployIfNotExists, AuditIfNotExists, Disabled 2.0.0 Configure Windows Arc Machines to be associated with a Data Collection Rule or a Data Collection Endpoint Deploy Association to link Windows Arc machines to the specified Data Collection Rule or the specified Data Collection Endpoint. The list of locations are updated over time as support is increased. DeployIfNotExists, Disabled 2.4.0 Configure Windows Arc-enabled machines to run Azure Monitor Agent Automate the deployment of Azure Monitor Agent extension on your Windows Arc-enabled machines for collecting telemetry data from the guest OS. This policy will install the extension if the OS and region are supported and system-assigned managed identity is enabled, and skip install otherwise. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 2.6.0 Configure Windows Machines to be associated with a Data Collection Rule or a Data Collection Endpoint Deploy Association to link Windows virtual machines, virtual machine scale sets, and Arc machines to the specified Data Collection Rule or the specified Data Collection Endpoint. The list of locations and OS images are updated over time as support is increased. DeployIfNotExists, Disabled 4.8.0 Configure Windows Virtual Machine Scale Sets to be associated with a Data Collection Rule or a Data Collection Endpoint Deploy Association to link Windows virtual machine scale sets to the specified Data Collection Rule or the specified Data Collection Endpoint. The list of locations and OS images are updated over time as support is increased. DeployIfNotExists, Disabled 3.7.0 Configure Windows virtual machine scale sets to run Azure Monitor Agent using system-assigned managed identity Automate the deployment of Azure Monitor Agent extension on your Windows virtual machine scale sets for collecting telemetry data from the guest OS. This policy will install the extension if the OS and region are supported and system-assigned managed identity is enabled, and skip install otherwise. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 3.7.0 Configure Windows virtual machine scale sets to run Azure Monitor Agent with user-assigned managed identity-based authentication Automate the deployment of Azure Monitor Agent extension on your Windows virtual machine scale sets for collecting telemetry data from the guest OS. This policy will install the extension and configure it to use the specified user-assigned managed identity if the OS and region are supported, and skip install otherwise. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 1.9.0 Configure Windows Virtual Machines to be associated with a Data Collection Rule or a Data Collection Endpoint Deploy Association to link Windows virtual machines to the specified Data Collection Rule or the specified Data Collection Endpoint. The list of locations and OS images are updated over time as support is increased. DeployIfNotExists, Disabled 3.6.0 Configure Windows virtual machines to run Azure Monitor Agent using system-assigned managed identity Automate the deployment of Azure Monitor Agent extension on your Windows virtual machines for collecting telemetry data from the guest OS. This policy will install the extension if the OS and region are supported and system-assigned managed identity is enabled, and skip install otherwise. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 4.7.0 Configure Windows virtual machines to run Azure Monitor Agent with user-assigned managed identity-based authentication Automate the deployment of Azure Monitor Agent extension on your Windows virtual machines for collecting telemetry data from the guest OS. This policy will install the extension and configure it to use the specified user-assigned managed identity if the OS and region are supported, and skip install otherwise. Learn more: https://aka.ms/AMAOverview. DeployIfNotExists, Disabled 1.9.0 Dependency agent should be enabled for listed virtual machine images Reports virtual machines as non-compliant if the virtual machine image is in the list defined and the agent is not installed. The list of OS images is updated over time as support is updated.

AuditIfNotExists, Disabled 2.1.0 Dependency agent should be enabled in virtual machine scale sets for listed virtual machine images Reports virtual machine scale sets as non-compliant if the virtual machine image is in the list defined and the agent is not installed. The list of OS images is updated over time as support is updated. AuditIfNotExists, Disabled 2.1.0 Deploy - Configure Dependency agent to be enabled on Windows virtual machine scale sets Deploy Dependency agent for Windows virtual machine scale sets if the virtual machine image is in the list defined and the agent is not installed. If your scale set upgradePolicy is set to Manual, you need to apply the extension to all the virtual machines in the set by updating them. DeployIfNotExists, Disabled 3.3.0 Deploy - Configure Dependency agent to be enabled on Windows virtual machines Deploy Dependency agent for Windows virtual machines if the virtual machine image is in the list defined and the agent is not installed. DeployIfNotExists, Disabled 3.3.0 Deploy - Configure diagnostic settings to a Log Analytics workspace to be enabled on Azure Key Vault Managed HSM Deploys the diagnostic settings for Azure Key Vault Managed HSM to stream to a regional Log Analytics workspace when any Azure Key Vault Managed HSM which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 1.0.0 Deploy Dependency agent for Linux virtual machine scale sets Deploy Dependency agent for Linux virtual machine scale sets if the VM Image (OS) is in the list defined and the agent is not installed. Note: if your scale set upgradePolicy is set to Manual, you need to apply the extension to the all virtual machines in the set by calling upgrade on them. In CLI this would be az vmss update-instances. deployIfNotExists 5.1.0 Deploy Dependency agent for Linux virtual machine scale sets with Azure Monitoring Agent settings Deploy Dependency agent for Linux virtual machine scale sets with Azure Monitoring Agent settings if the VM Image (OS) is in the list defined and the agent is not installed. Note: if your scale set upgradePolicy is set to Manual, you need to apply the extension to the all virtual machines in the set by calling upgrade on them. In CLI this would be az vmss update-instances. DeployIfNotExists, Disabled 3.2.0 Deploy Dependency agent for Linux virtual machines Deploy Dependency agent for Linux virtual machines if the VM Image (OS) is in the list defined and the agent is not installed. deployIfNotExists 5.1.0 Deploy Dependency agent for Linux virtual machines with Azure Monitoring Agent settings Deploy Dependency agent for Linux virtual machines with Azure Monitoring Agent settings if the VM Image (OS) is in the list defined and the agent is not installed. DeployIfNotExists, Disabled 3.2.0 Deploy Dependency agent to be enabled on Windows virtual machine scale sets with Azure Monitoring Agent settings Deploy Dependency agent for Windows virtual machine scale sets with Azure Monitoring Agent settings if the virtual machine image is in the list defined and the agent is not installed. If your scale set upgradePolicy is set to Manual, you need to apply the extension to all the virtual machines in the set by updating them. DeployIfNotExists, Disabled 1.4.0 Deploy Dependency agent to be enabled on Windows virtual machines with Azure Monitoring Agent settings Deploy Dependency agent for Windows virtual machines with Azure Monitoring Agent settings if the virtual machine image is in the list defined and the agent is not installed. DeployIfNotExists, Disabled 1.4.0 Deploy Diagnostic Settings for Batch Account to Event Hub Deploys the diagnostic settings for Batch Account to stream to a regional Event Hub when any Batch Account which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.0.0 Deploy Diagnostic Settings for Batch Account to Log Analytics workspace Deploys the diagnostic settings for Batch Account to stream to a regional Log Analytics workspace when any Batch Account which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 1.1.0 Deploy Diagnostic Settings for Data Lake Analytics to Event Hub Deploys the diagnostic settings for Data Lake Analytics to stream to a regional Event Hub when any Data Lake Analytics which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.0.0 Deploy Diagnostic Settings for Data Lake Analytics to Log Analytics workspace Deploys the diagnostic settings for Data Lake Analytics to stream to a regional Log Analytics

workspace when any Data Lake Analytics which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 1.0.0 Deploy Diagnostic Settings for Data Lake Storage Gen1 to Event Hub Deploys the diagnostic settings for Data Lake Storage Gen1 to stream to a regional Event Hub when any Data Lake Storage Gen1 which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.0.0 Deploy Diagnostic Settings for Data Lake Storage Gen1 to Log Analytics workspace Deploys the diagnostic settings for Data Lake Storage Gen1 to stream to a regional Log Analytics workspace when any Data Lake Storage Gen1 which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 1.0.0 Deploy Diagnostic Settings for Event Hub to Event Hub Deploys the diagnostic settings for Event Hub to stream to a regional Event Hub when any Event Hub which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.1.0 Deploy Diagnostic Settings for Event Hub to Log Analytics workspace Deploys the diagnostic settings for Event Hub to stream to a regional Log Analytics workspace when any Event Hub which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.3.0 Deploy Diagnostic Settings for Key Vault to Log Analytics workspace Deploys the diagnostic settings for Key Vault to stream to a regional Log Analytics workspace when any Key Vault which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 3.0.0 Deploy Diagnostic Settings for Logic Apps to Event Hub Deploys the diagnostic settings for Logic Apps to stream to a regional Event Hub when any Logic Apps which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.0.0 Deploy Diagnostic Settings for Logic Apps to Log Analytics workspace Deploys the diagnostic settings for Logic Apps to stream to a regional Log Analytics workspace when any Logic Apps which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 1.0.0 Deploy Diagnostic Settings for Network Security Groups This policy automatically deploys diagnostic settings to network security groups. A storage account with name '{storagePrefixParameter}{NSGLocation}' will be automatically created. deployIfNotExists 2.0.1 Deploy Diagnostic Settings for Search Services to Event Hub Deploys the diagnostic settings for Search Services to stream to a regional Event Hub when any Search Services which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.0.0 Deploy Diagnostic Settings for Search Services to Log Analytics workspace Deploys the diagnostic settings for Search Services to stream to a regional Log Analytics workspace when any Search Services which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 1.0.0 Deploy Diagnostic Settings for Service Bus to Event Hub Deploys the diagnostic settings for Service Bus to stream to a regional Event Hub when any Service Bus which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.0.0 Deploy Diagnostic Settings for Service Bus to Log Analytics workspace Deploys the diagnostic settings for Service Bus to stream to a regional Log Analytics workspace when any Service Bus which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.3.0 Deploy Diagnostic Settings for Stream Analytics to Event Hub Deploys the diagnostic settings for Stream Analytics to stream to a regional Event Hub when any Stream Analytics which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 2.0.0 Deploy Diagnostic Settings for Stream Analytics to Log Analytics workspace Deploys the diagnostic settings for Stream Analytics to stream to a regional Log Analytics workspace when any Stream Analytics which is missing this diagnostic settings is created or updated. DeployIfNotExists, Disabled 1.0.0 Enable logging by category group for 1ES Hosted Pools (microsoft.cloudtest/hostedpools) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for 1ES Hosted Pools (microsoft.cloudtest/hostedpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by

category group for 1ES Hosted Pools (microsoft.cloudtest/hostedpools) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for 1ES Hosted Pools (microsoft.cloudtest/hostedpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for 1ES Hosted Pools (microsoft.cloudtest/hostedpools) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for 1ES Hosted Pools (microsoft.cloudtest/hostedpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Analysis Services (microsoft.analysisservices/servers) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Analysis Services (microsoft.analysisservices/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Analysis Services (microsoft.analysisservices/servers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Analysis Services (microsoft.analysisservices/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Analysis Services (microsoft.analysisservices/servers) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Analysis Services (microsoft.analysisservices/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Apache Spark pools (microsoft.synapse/workspaces/bigdatapools) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Apache Spark pools (microsoft.synapse/workspaces/bigdatapools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Apache Spark pools (microsoft.synapse/workspaces/bigdatapools) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Apache Spark pools (microsoft.synapse/workspaces/bigdatapools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Apache Spark pools (microsoft.synapse/workspaces/bigdatapools) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Apache Spark pools (microsoft.synapse/workspaces/bigdatapools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for API Management services (microsoft.apimanagement/service) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for API Management services (microsoft.apimanagement/service). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for API Management services (microsoft.apimanagement/service) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and

insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for API Management services (microsoft.apimanagement/service). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for API Management services (microsoft.apimanagement/service) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for API Management services (microsoft.apimanagement/service). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for App Configuration (microsoft.appconfiguration/configurationstores) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for App Configuration (microsoft.appconfiguration/configurationstores). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for App Configuration (microsoft.appconfiguration/configurationstores) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for App Configuration (microsoft.appconfiguration/configurationstores). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for App Configuration (microsoft.appconfiguration/configurationstores) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for App Configuration (microsoft.appconfiguration/configurationstores). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for App Service (microsoft.web/sites) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for App Service (microsoft.web/sites). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for App Service Environments (microsoft.web/hostingenvironments) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for App Service Environments (microsoft.web/hostingenvironments). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for App Service Environments (microsoft.web/hostingenvironments) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for App Service Environments (microsoft.web/hostingenvironments). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for App Service Environments (microsoft.web/hostingenvironments) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for App Service Environments (microsoft.web/hostingenvironments). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application gateways (microsoft.network/applicationgateways) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group

to route logs to an Event Hub for Application gateways (microsoft.network/applicationgateways). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application gateways (microsoft.network/applicationgateways) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Application gateways (microsoft.network/applicationgateways). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application gateways (microsoft.network/applicationgateways) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Application gateways (microsoft.network/applicationgateways). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application group (microsoft.desktopvirtualization/applicationgroups) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Virtual Desktop Application group (microsoft.desktopvirtualization/applicationgroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application groups (microsoft.desktopvirtualization/applicationgroups) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Application groups (microsoft.desktopvirtualization/applicationgroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application groups (microsoft.desktopvirtualization/applicationgroups) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Application groups (microsoft.desktopvirtualization/applicationgroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application groups (microsoft.desktopvirtualization/applicationgroups) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Application groups (microsoft.desktopvirtualization/applicationgroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application Insights (microsoft.insights/components) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Application Insights (microsoft.insights/components). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application Insights (microsoft.insights/components) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Application Insights (microsoft.insights/components). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Application Insights (Microsoft.Insights/components) to Log Analytics (Virtual Enclaves) Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group

to route logs to a Log Analytics workspace for Application Insights (Microsoft.Insights/components). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.1 Enable logging by category group for Application Insights (microsoft.insights/components) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Application Insights (microsoft.insights/components). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Attestation providers (microsoft.attestation/attestationproviders) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Attestation providers (microsoft.attestation/attestationproviders). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Attestation providers (microsoft.attestation/attestationproviders) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Attestation providers (microsoft.attestation/attestationproviders). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Attestation providers (microsoft.attestation/attestationproviders) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Attestation providers (microsoft.attestation/attestationproviders). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Automation Accounts (microsoft.automation/automationaccounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Automation Accounts (microsoft.automation/automationaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Automation Accounts (microsoft.automation/automationaccounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Automation Accounts (microsoft.automation/automationaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Automation Accounts (microsoft.automation/automationaccounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Automation Accounts (microsoft.automation/automationaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for AVS Private clouds (microsoft.avs/privateclouds) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for AVS Private clouds (microsoft.avs/privateclouds). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for AVS Private clouds (microsoft.avs/privateclouds) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for AVS Private clouds (microsoft.avs/privateclouds). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for AVS Private clouds

(microsoft.avs/privateclouds) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for AVS Private clouds (microsoft.avs/privateclouds). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Azure AD Domain Services (microsoft.aad/domainservices) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure AD Domain Services (microsoft.aad/domainservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure AD Domain Services (microsoft.aad/domainservices) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure AD Domain Services (microsoft.aad/domainservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure AD Domain Services (microsoft.aad/domainservices) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure AD Domain Services (microsoft.aad/domainservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure API for FHIR (microsoft.healthcareapis/services) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure API for FHIR (microsoft.healthcareapis/services). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure API for FHIR (microsoft.healthcareapis/services) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure API for FHIR (microsoft.healthcareapis/services). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure API for FHIR (microsoft.healthcareapis/services) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure API for FHIR (microsoft.healthcareapis/services). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Cache for Redis (microsoft.cache/redis) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Cache for Redis (microsoft.cache/redis). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Azure Cache for Redis (microsoft.cache/redis) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Cache for Redis (microsoft.cache/redis). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Azure Cache for Redis (microsoft.cache/redis) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Cache for Redis

(microsoft.cache/redis). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Azure Cosmos DB (microsoft.documentdb/databaseaccounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Cosmos DB (microsoft.documentdb/databaseaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Cosmos DB accounts (microsoft.documentdb/databaseaccounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Cosmos DB accounts (microsoft.documentdb/databaseaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Cosmos DB accounts (microsoft.documentdb/databaseaccounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Cosmos DB accounts (microsoft.documentdb/databaseaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Cosmos DB accounts (microsoft.documentdb/databaseaccounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Cosmos DB accounts (microsoft.documentdb/databaseaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Data Explorer Clusters (microsoft.kusto/clusters) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Data Explorer Clusters (microsoft.kusto/clusters). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Data Explorer Clusters (microsoft.kusto/clusters) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Data Explorer Clusters (microsoft.kusto/clusters). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Data Explorer Clusters (microsoft.kusto/clusters) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Data Explorer Clusters (microsoft.kusto/clusters). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Database for MariaDB servers (microsoft.dbformariadb/servers) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Database for MariaDB servers (microsoft.dbformariadb/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Database for MariaDB servers (microsoft.dbformariadb/servers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Database for MariaDB servers (microsoft.dbformariadb/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0

Enable logging by category group for Azure Database for MariaDB servers (microsoft.dbformariadb/servers) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Database for MariaDB servers (microsoft.dbformariadb/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Database for MySQL servers (microsoft.dbformysql/servers) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Database for MySQL servers (microsoft.dbformysql/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Database for MySQL servers (microsoft.dbformysql/servers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Database for MySQL servers (microsoft.dbformysql/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Database for MySQL servers (microsoft.dbformysql/servers) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Database for MySQL servers (microsoft.dbformysql/servers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Databricks Services (microsoft.databricks/workspaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Databricks Services (microsoft.databricks/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Databricks Services (microsoft.databricks/workspaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Databricks Services (microsoft.databricks/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Databricks Services (microsoft.databricks/workspaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Databricks Services (microsoft.databricks/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Digital Twins (microsoft.digitaltwins/digitaltwinsinstances) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Digital Twins (microsoft.digitaltwins/digitaltwinsinstances). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Digital Twins (microsoft.digitaltwins/digitaltwinsinstances) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Digital Twins (microsoft.digitaltwins/digitaltwinsinstances). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Digital Twins (microsoft.digitaltwins/digitaltwinsinstances) to

Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Digital Twins (microsoft.digitaltwins/digitaltwinsinstances). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure FarmBeats (microsoft.agfoodplatform/farmbeats) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure FarmBeats (microsoft.agfoodplatform/farmbeats). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Azure FarmBeats (microsoft.agfoodplatform/farmbeats) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure FarmBeats (microsoft.agfoodplatform/farmbeats). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Azure FarmBeats (microsoft.agfoodplatform/farmbeats) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure FarmBeats (microsoft.agfoodplatform/farmbeats). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Azure Load Testing (microsoft.loadtestservice/loadtests) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Load Testing (microsoft.loadtestservice/loadtests). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Load Testing (microsoft.loadtestservice/loadtests) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Load Testing (microsoft.loadtestservice/loadtests). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Load Testing (microsoft.loadtestservice/loadtests) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Load Testing (microsoft.loadtestservice/loadtests). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Machine Learning (microsoft.machinelearningservices/workspaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Machine Learning (microsoft.machinelearningservices/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Azure Machine Learning (microsoft.machinelearningservices/workspaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Machine Learning (microsoft.machinelearningservices/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Azure Machine Learning (microsoft.machinelearningservices/workspaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This

policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Machine Learning (microsoft.machinelearningservices/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Azure Managed Grafana (microsoft.dashboard/grafana) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Managed Grafana (microsoft.dashboard/grafana). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Managed Grafana (microsoft.dashboard/grafana) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Managed Grafana (microsoft.dashboard/grafana). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Managed Grafana (microsoft.dashboard/grafana) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Managed Grafana (microsoft.dashboard/grafana). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Spring Apps (microsoft.appplatform/spring) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Spring Apps (microsoft.appplatform/spring). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Spring Apps (microsoft.appplatform/spring) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Spring Apps (microsoft.appplatform/spring). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Spring Apps (microsoft.appplatform/spring) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Spring Apps (microsoft.appplatform/spring). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Synapse Analytics (microsoft.synapse/workspaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Synapse Analytics (microsoft.synapse/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Synapse Analytics (microsoft.synapse/workspaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Synapse Analytics (microsoft.synapse/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Synapse Analytics (microsoft.synapse/workspaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Synapse Analytics (microsoft.synapse/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Video Indexer (microsoft.videoindexer/accounts) to Event Hub Resource logs should

be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Azure Video Indexer (microsoft.videoindexer/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Video Indexer (microsoft.videoindexer/accounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Video Indexer (microsoft.videoindexer/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Azure Video Indexer (microsoft.videoindexer/accounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Azure Video Indexer (microsoft.videoindexer/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Backup vaults (microsoft.dataprotection/backupvaults) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Backup vaults (microsoft.dataprotection/backupvaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Backup vaults (microsoft.dataprotection/backupvaults) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Backup vaults (microsoft.dataprotection/backupvaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Backup vaults (microsoft.dataprotection/backupvaults) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Backup vaults (microsoft.dataprotection/backupvaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Bastions (microsoft.network/bastionhosts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Bastions (microsoft.network/bastionhosts). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Bastions (microsoft.network/bastionhosts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Bastions (microsoft.network/bastionhosts). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Bastions (microsoft.network/bastionhosts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Bastions (microsoft.network/bastionhosts). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Batch accounts (microsoft.batch/batchaccounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Batch accounts (microsoft.batch/batchaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category

group for Batch accounts (microsoft.batch/batchaccounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Batch accounts (microsoft.batch/batchaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Batch accounts (microsoft.batch/batchaccounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Batch accounts (microsoft.batch/batchaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Bot Services (microsoft.botservice/botservices) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Bot Services (microsoft.botservice/botservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Bot Services (microsoft.botservice/botservices) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Bot Services (microsoft.botservice/botservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Bot Services (microsoft.botservice/botservices) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Bot Services (microsoft.botservice/botservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Caches (microsoft.cache/redisenterprise/databases) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Caches (microsoft.cache/redisenterprise/databases). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Caches (microsoft.cache/redisenterprise/databases) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Caches (microsoft.cache/redisenterprise/databases). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Caches (microsoft.cache/redisenterprise/databases) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Caches (microsoft.cache/redisenterprise/databases). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Chaos Experiments (microsoft.chaos/experiments) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Chaos Experiments (microsoft.chaos/experiments). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Chaos Experiments (microsoft.chaos/experiments) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Chaos Experiments (microsoft.chaos/experiments).

DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Chaos Experiments (microsoft.chaos/experiments) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Chaos Experiments (microsoft.chaos/experiments). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Code Signing Accounts (microsoft.codesigning/codesigningaccounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Code Signing Accounts (microsoft.codesigning/codesigningaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Code Signing Accounts (microsoft.codesigning/codesigningaccounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Code Signing Accounts (microsoft.codesigning/codesigningaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Code Signing Accounts (microsoft.codesigning/codesigningaccounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Code Signing Accounts (microsoft.codesigning/codesigningaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Cognitive Services (microsoft.cognitiveservices/accounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Cognitive Services (microsoft.cognitiveservices/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Cognitive Services (microsoft.cognitiveservices/accounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Cognitive Services (microsoft.cognitiveservices/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Cognitive Services (microsoft.cognitiveservices/accounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Cognitive Services (microsoft.cognitiveservices/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Communication Services (microsoft.communication/communicationservices) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Communication Services (microsoft.communication/communicationservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Communication Services (microsoft.communication/communicationservices) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Communication Services (microsoft.communication/communicationservices). DeployIfNotExists,

AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Communication Services (microsoft.communication/communicationservices) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Communication Services (microsoft.communication/communicationservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Connected Cache Resources (microsoft.connectedcache/ispcustomers) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Connected Cache Resources (microsoft.connectedcache/ispcustomers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Connected Cache Resources (microsoft.connectedcache/ispcustomers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Connected Cache Resources (microsoft.connectedcache/ispcustomers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Connected Cache Resources (microsoft.connectedcache/ispcustomers) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Connected Cache Resources (microsoft.connectedcache/ispcustomers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Container Apps Environments (microsoft.app/managedenvironments) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Container Apps Environments (microsoft.app/managedenvironments). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Container Apps Environments (microsoft.app/managedenvironments) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Container Apps Environments (microsoft.app/managedenvironments). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Container Apps Environments (microsoft.app/managedenvironments) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Container Apps Environments (microsoft.app/managedenvironments). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Container instances (microsoft.containerinstance/containergroups) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Container instances (microsoft.containerinstance/containergroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Container instances (microsoft.containerinstance/containergroups) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Container instances (microsoft.containerinstance/containergroups).

DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Container instances (microsoft.containerinstance/containergroups) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Container instances (microsoft.containerinstance/containergroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Container registries (microsoft.containerregistry/registries) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Container registries (microsoft.containerregistry/registries). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Container registries (microsoft.containerregistry/registries) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Container registries (microsoft.containerregistry/registries). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Container registries (microsoft.containerregistry/registries) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Container registries (microsoft.containerregistry/registries). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Data collection rules (microsoft.insights/datacollectionrules) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Data collection rules (microsoft.insights/datacollectionrules). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data collection rules (microsoft.insights/datacollectionrules) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Data collection rules (microsoft.insights/datacollectionrules). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data collection rules (microsoft.insights/datacollectionrules) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Data collection rules (microsoft.insights/datacollectionrules). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data factories (V2) (microsoft.datafactory/factories) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Data factories (V2) (microsoft.datafactory/factories). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data factories (V2) (microsoft.datafactory/factories) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Data factories (V2) (microsoft.datafactory/factories). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data factories (V2) (microsoft.datafactory/factories) to Storage Resource logs should be enabled to track activities and events that

take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Data factories (V2) (microsoft.datafactory/factories). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Lake Analytics (microsoft.datalakeanalytics/accounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Data Lake Analytics (microsoft.datalakeanalytics/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Lake Analytics (microsoft.datalakeanalytics/accounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Data Lake Analytics (microsoft.datalakeanalytics/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Lake Analytics (microsoft.datalakeanalytics/accounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Data Lake Analytics (microsoft.datalakeanalytics/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Lake Storage Gen1 (microsoft.datalakestore/accounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Data Lake Storage Gen1 (microsoft.datalakestore/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Lake Storage Gen1 (microsoft.datalakestore/accounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Data Lake Storage Gen1 (microsoft.datalakestore/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Lake Storage Gen1 (microsoft.datalakestore/accounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Data Lake Storage Gen1 (microsoft.datalakestore/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Shares (microsoft.datashare/accounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Data Shares (microsoft.datashare/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Shares (microsoft.datashare/accounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Data Shares (microsoft.datashare/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Data Shares (microsoft.datashare/accounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Data Shares (microsoft.datashare/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0

Enable logging by category group for Dedicated SQL pools (microsoft.synapse/workspaces/sqlpools) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Dedicated SQL pools (microsoft.synapse/workspaces/sqlpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Dedicated SQL pools (microsoft.synapse/workspaces/sqlpools) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Dedicated SQL pools (microsoft.synapse/workspaces/sqlpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Dedicated SQL pools (microsoft.synapse/workspaces/sqlpools) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Dedicated SQL pools (microsoft.synapse/workspaces/sqlpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Dev centers (microsoft.devcenter/devcenters) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Dev centers (microsoft.devcenter/devcenters). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Dev centers (microsoft.devcenter/devcenters) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Dev centers (microsoft.devcenter/devcenters). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Dev centers (microsoft.devcenter/devcenters) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Dev centers (microsoft.devcenter/devcenters). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for DICOM service (microsoft.healthcareapis/workspaces/dicomservices) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for DICOM service (microsoft.healthcareapis/workspaces/dicomservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for DICOM service (microsoft.healthcareapis/workspaces/dicomservices) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for DICOM service (microsoft.healthcareapis/workspaces/dicomservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for DICOM service (microsoft.healthcareapis/workspaces/dicomservices) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for DICOM service (microsoft.healthcareapis/workspaces/dicomservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Endpoints (microsoft.cdn/profiles/endpoints) to Event Hub Resource logs

should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Endpoints (microsoft.cdn/profiles/endpoints). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Endpoints (microsoft.cdn/profiles/endpoints) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Endpoints (microsoft.cdn/profiles/endpoints). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Endpoints (microsoft.cdn/profiles/endpoints) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Endpoints (microsoft.cdn/profiles/endpoints). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Event Grid Domains (microsoft.eventgrid/domains) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Event Grid Domains (microsoft.eventgrid/domains). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Event Grid Domains (microsoft.eventgrid/domains) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Event Grid Domains (microsoft.eventgrid/domains). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Event Grid Domains (microsoft.eventgrid/domains) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Event Grid Domains (microsoft.eventgrid/domains). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Event Grid Partner Namespaces (microsoft.eventgrid/partnernamespaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Event Grid Partner Namespaces (microsoft.eventgrid/partnernamespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Event Grid Partner Namespaces (microsoft.eventgrid/partnernamespaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Event Grid Partner Namespaces (microsoft.eventgrid/partnernamespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Event Grid Partner Namespaces (microsoft.eventgrid/partnernamespaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Event Grid Partner Namespaces (microsoft.eventgrid/partnernamespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Event Grid Partner Topics (microsoft.eventgrid/partnertopics) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group

to route logs to an Event Hub for Event Grid Partner Topics (microsoft.eventgrid/partnertopics). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Event Grid Partner Topics (microsoft.eventgrid/partnertopics) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Event Grid Partner Topics (microsoft.eventgrid/partnertopics). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Event Grid Partner Topics (microsoft.eventgrid/partnertopics) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Event Grid Partner Topics (microsoft.eventgrid/partnertopics). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Event Grid System Topics (microsoft.eventgrid/systemtopics) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Event Grid System Topics (microsoft.eventgrid/systemtopics). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Event Grid System Topics (microsoft.eventgrid/systemtopics) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Event Grid System Topics (microsoft.eventgrid/systemtopics). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Event Grid System Topics (microsoft.eventgrid/systemtopics) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Event Grid System Topics (microsoft.eventgrid/systemtopics). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Event Grid Topics (microsoft.eventgrid/topics) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Event Grid Topics (microsoft.eventgrid/topics). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Event Grid Topics (microsoft.eventgrid/topics) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Event Grid Topics (microsoft.eventgrid/topics). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Event Grid Topics (microsoft.eventgrid/topics) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Event Grid Topics (microsoft.eventgrid/topics). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Event Hubs Namespaces (microsoft.eventhub/namespaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Event Hubs Namespaces (microsoft.eventhub/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Event Hubs Namespaces (microsoft.eventhub/namespaces) to Log

Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Event Hubs Namespaces (microsoft.eventhub/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Event Hubs Namespaces (microsoft.eventhub/namespaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Event Hubs Namespaces (microsoft.eventhub/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Experiment Workspaces (microsoft.experimentation/experimentworkspaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Experiment Workspaces (microsoft.experimentation/experimentworkspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Experiment Workspaces (microsoft.experimentation/experimentworkspaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Experiment Workspaces (microsoft.experimentation/experimentworkspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Experiment Workspaces (microsoft.experimentation/experimentworkspaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Experiment Workspaces (microsoft.experimentation/experimentworkspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for ExpressRoute circuits (microsoft.network/expressroutecircuits) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for ExpressRoute circuits (microsoft.network/expressroutecircuits). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for ExpressRoute circuits (microsoft.network/expressroutecircuits) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for ExpressRoute circuits (microsoft.network/expressroutecircuits). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for ExpressRoute circuits (microsoft.network/expressroutecircuits) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for ExpressRoute circuits (microsoft.network/expressroutecircuits). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for FHIR service (microsoft.healthcareapis/workspaces/fhirservices) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for FHIR service (microsoft.healthcareapis/workspaces/fhirservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for FHIR service (microsoft.healthcareapis/workspaces/fhirservices) to Log

Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for FHIR service (microsoft.healthcareapis/workspaces/fhirservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for FHIR service (microsoft.healthcareapis/workspaces/fhirservices) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for FHIR service (microsoft.healthcareapis/workspaces/fhirservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Firewall (microsoft.network/azurefirewalls) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Firewall (microsoft.network/azurefirewalls). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Firewalls (microsoft.network/azurefirewalls) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Firewalls (microsoft.network/azurefirewalls). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Firewalls (microsoft.network/azurefirewalls) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Firewalls (microsoft.network/azurefirewalls). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Firewalls (microsoft.network/azurefirewalls) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Firewalls (microsoft.network/azurefirewalls). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Front Door and CDN profiles (microsoft.cdn/profiles) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Front Door and CDN profiles (microsoft.cdn/profiles). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Front Door and CDN profiles (microsoft.cdn/profiles) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Front Door and CDN profiles (microsoft.cdn/profiles). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Front Door and CDN profiles (microsoft.cdn/profiles) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Front Door and CDN profiles (microsoft.cdn/profiles). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Front Door and CDN profiles (microsoft.network/frontdoors) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Front Door and CDN

profiles (microsoft.network/frontdoors). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Front Door and CDN profiles (microsoft.network/frontdoors) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Front Door and CDN profiles (microsoft.network/frontdoors). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Front Door and CDN profiles (microsoft.network/frontdoors) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Front Door and CDN profiles (microsoft.network/frontdoors). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Function App (microsoft.web/sites) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Function App (microsoft.web/sites). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Host pool (microsoft.desktopvirtualization/hostpools) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Virtual Desktop Host pool (microsoft.desktopvirtualization/hostpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Host pools (microsoft.desktopvirtualization/hostpools) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Host pools (microsoft.desktopvirtualization/hostpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Host pools (microsoft.desktopvirtualization/hostpools) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Host pools (microsoft.desktopvirtualization/hostpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Host pools (microsoft.desktopvirtualization/hostpools) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Host pools (microsoft.desktopvirtualization/hostpools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for HPC caches (microsoft.storagecache/caches) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for HPC caches (microsoft.storagecache/caches). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for HPC caches (microsoft.storagecache/caches) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for HPC caches (microsoft.storagecache/caches). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for HPC caches (microsoft.storagecache/caches) to Storage Resource logs should be enabled to track activities and events that take

place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for HPC caches (microsoft.storagecache/caches). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Integration accounts (microsoft.logic/integrationaccounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Integration accounts (microsoft.logic/integrationaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Integration accounts (microsoft.logic/integrationaccounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Integration accounts (microsoft.logic/integrationaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Integration accounts (microsoft.logic/integrationaccounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Integration accounts (microsoft.logic/integrationaccounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for IoT Hub (microsoft.devices/iothubs) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for IoT Hub (microsoft.devices/iothubs). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for IoT Hub (microsoft.devices/iothubs) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for IoT Hub (microsoft.devices/iothubs). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for IoT Hub (microsoft.devices/iothubs) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for IoT Hub (microsoft.devices/iothubs). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Key vaults (microsoft.keyvault/vaults) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Key vaults (microsoft.keyvault/vaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Key vaults (microsoft.keyvault/vaults) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Key vaults (microsoft.keyvault/vaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Key vaults (microsoft.keyvault/vaults) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Key vaults (microsoft.keyvault/vaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Live events (microsoft.media/mediaservices/liveevents) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any

changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Live events (microsoft.media/mediaservices/liveevents). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Live events (microsoft.media/mediaservices/liveevents) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Live events (microsoft.media/mediaservices/liveevents). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Live events (microsoft.media/mediaservices/liveevents) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Live events (microsoft.media/mediaservices/liveevents). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Load balancers (microsoft.network/loadbalancers) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Load balancers (microsoft.network/loadbalancers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Load balancers (microsoft.network/loadbalancers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Load balancers (microsoft.network/loadbalancers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Load balancers (microsoft.network/loadbalancers) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Load balancers (microsoft.network/loadbalancers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Log Analytics workspaces (microsoft.operationalinsights/workspaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Log Analytics workspaces (microsoft.operationalinsights/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Log Analytics workspaces (microsoft.operationalinsights/workspaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Log Analytics workspaces (microsoft.operationalinsights/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Log Analytics workspaces (microsoft.operationalinsights/workspaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Log Analytics workspaces (microsoft.operationalinsights/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Logic apps (microsoft.logic/workflows) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Logic apps (microsoft.logic/workflows). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by

category group for Logic apps (microsoft.logic/workflows) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Logic apps (microsoft.logic/workflows). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Logic apps (microsoft.logic/workflows) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Logic apps (microsoft.logic/workflows). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Managed CCF Apps (microsoft.confidentialledger/managedccfs) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Managed CCF Apps (microsoft.confidentialledger/managedccfs). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Managed CCF Apps (microsoft.confidentialledger/managedccfs) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Managed CCF Apps (microsoft.confidentialledger/managedccfs). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Managed CCF Apps (microsoft.confidentialledger/managedccfs) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Managed CCF Apps (microsoft.confidentialledger/managedccfs). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Managed databases (microsoft.sql/managedinstances/databases) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Managed databases (microsoft.sql/managedinstances/databases). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Managed databases (microsoft.sql/managedinstances/databases) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Managed databases (microsoft.sql/managedinstances/databases). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Managed databases (microsoft.sql/managedinstances/databases) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Managed databases (microsoft.sql/managedinstances/databases). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Managed HSMs (microsoft.keyvault/managedhsms) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Managed HSMs (microsoft.keyvault/managedhsms). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Managed HSMs (microsoft.keyvault/managedhsms) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category

group to route logs to a Log Analytics workspace for Managed HSMs (microsoft.keyvault/managedhsms). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Managed HSMs (microsoft.keyvault/managedhsms) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Managed HSMs (microsoft.keyvault/managedhsms). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Media Services (microsoft.media/mediaservices) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Media Services (microsoft.media/mediaservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Media Services (microsoft.media/mediaservices) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Media Services (microsoft.media/mediaservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Media Services (microsoft.media/mediaservices) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Media Services (microsoft.media/mediaservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for MedTech service (microsoft.healthcareapis/workspaces/iotconnectors) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for MedTech service (microsoft.healthcareapis/workspaces/iotconnectors). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for MedTech service (microsoft.healthcareapis/workspaces/iotconnectors) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for MedTech service (microsoft.healthcareapis/workspaces/iotconnectors). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for MedTech service (microsoft.healthcareapis/workspaces/iotconnectors) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for MedTech service (microsoft.healthcareapis/workspaces/iotconnectors). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Microsoft Purview accounts (microsoft.purview/accounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Microsoft Purview accounts (microsoft.purview/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Microsoft Purview accounts (microsoft.purview/accounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Microsoft Purview accounts (microsoft.purview/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by

category group for Microsoft Purview accounts (microsoft.purview/accounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Microsoft Purview accounts (microsoft.purview/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for microsoft.autonomousdevelopmentplatform/workspaces to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.autonomousdevelopmentplatform/workspaces. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.autonomousdevelopmentplatform/workspaces to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.autonomousdevelopmentplatform/workspaces. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.autonomousdevelopmentplatform/workspaces to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.autonomousdevelopmentplatform/workspaces. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.azuresphere/catalogs to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.azuresphere/catalogs. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.azuresphere/catalogs to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.azuresphere/catalogs. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.azuresphere/catalogs to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.azuresphere/catalogs. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.cdn/cdnwebapplicationfirewallpolicies to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.cdn/cdnwebapplicationfirewallpolicies. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.cdn/cdnwebapplicationfirewallpolicies to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.cdn/cdnwebapplicationfirewallpolicies. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.cdn/cdnwebapplicationfirewallpolicies to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for

microsoft.cdn/cdnwebapplicationfirewallpolicies. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.classicnetwork/networksecuritygroups to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.classicnetwork/networksecuritygroups. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.classicnetwork/networksecuritygroups to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.classicnetwork/networksecuritygroups. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.classicnetwork/networksecuritygroups to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.classicnetwork/networksecuritygroups. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.community/communitytrainings to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.community/communitytrainings. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.community/communitytrainings to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.community/communitytrainings. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.community/communitytrainings to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.community/communitytrainings. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.connectedcache/enterprisemcccustomers to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.connectedcache/enterprisemcccustomers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.connectedcache/enterprisemcccustomers to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.connectedcache/enterprisemcccustomers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.connectedcache/enterprisemcccustomers to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.connectedcache/enterprisemcccustomers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.custompproviders/resourceproviders to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into

any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.customproviders/resourceproviders. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.customproviders/resourceproviders to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.customproviders/resourceproviders. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.customproviders/resourceproviders to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.customproviders/resourceproviders. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.d365customerinsights/instances to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.d365customerinsights/instances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.d365customerinsights/instances to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.d365customerinsights/instances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.d365customerinsights/instances to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.d365customerinsights/instances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbformysql/flexibleservers to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.dbformysql/flexibleservers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbformysql/flexibleservers to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.dbformysql/flexibleservers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbformysql/flexibleservers to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.dbformysql/flexibleservers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/flexibleservers to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.dbforpostgresql/flexibleservers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/flexibleservers to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes

that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.dbforpostgresql/flexibleservers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/flexibleservers to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.dbforpostgresql/flexibleservers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/servergroupsv2 to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.dbforpostgresql/servergroupsv2. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/servergroupsv2 to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.dbforpostgresql/servergroupsv2. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/servergroupsv2 to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.dbforpostgresql/servergroupsv2. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/servers to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.dbforpostgresql/servers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/servers to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.dbforpostgresql/servers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.dbforpostgresql/servers to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.dbforpostgresql/servers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.devices/provisioningservices to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.devices/provisioningservices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.devices/provisioningservices to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.devices/provisioningservices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.devices/provisioningservices to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage

Account for microsoft.devices/provisioningservices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.documentdb/cassandraclusters to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.documentdb/cassandraclusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.documentdb/cassandraclusters to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.documentdb/cassandraclusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.documentdb/cassandraclusters to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.documentdb/cassandraclusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.documentdb/mongoclusters to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.documentdb/mongoclusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.documentdb/mongoclusters to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.documentdb/mongoclusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.documentdb/mongoclusters to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.documentdb/mongoclusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.insights/autoscalesettings to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.insights/autoscalesettings. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.insights/autoscalesettings to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.insights/autoscalesettings. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.insights/autoscalesettings to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.insights/autoscalesettings. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.machinelearningservices/registries to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.machinelearningservices/registries. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.machinelearningservices/registries to Log Analytics Resource logs should

be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.machinelearningservices/registries. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.machinelearningservices/registries to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.machinelearningservices/registries. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.machinelearningservices/workspaces/onlineendpoints to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.machinelearningservices/workspaces/onlineendpoints. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.machinelearningservices/workspaces/onlineendpoints to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.machinelearningservices/workspaces/onlineendpoints. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.machinelearningservices/workspaces/onlineendpoints to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.machinelearningservices/workspaces/onlineendpoints. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.managednetworkfabric/networkdevices to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.managednetworkfabric/networkdevices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.managednetworkfabric/networkdevices to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.managednetworkfabric/networkdevices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.managednetworkfabric/networkdevices to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.managednetworkfabric/networkdevices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/dnsresolverpolicies to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.network/dnsresolverpolicies. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/dnsresolverpolicies to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics

workspace for microsoft.network/dnsresolverpolicies. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/dnsresolverpolicies to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.network/dnsresolverpolicies. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/networkmanagers/ipampools to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.network/networkmanagers/ipampools. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/networkmanagers/ipampools to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.network/networkmanagers/ipampools. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/networkmanagers/ipampools to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.network/networkmanagers/ipampools. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/networksecurityperimeters to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.network/networksecurityperimeters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/networksecurityperimeters to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.network/networksecurityperimeters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/networksecurityperimeters to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.network/networksecurityperimeters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/p2svpngateways to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.network/p2svpngateways. DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for microsoft.network/p2svpngateways to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.network/p2svpngateways. DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for microsoft.network/p2svpngateways to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for

microsoft.network/p2svpngateways. DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for microsoft.network/vpngateways to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.network/vpngateways. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/vpngateways to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.network/vpngateways. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.network/vpngateways to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.network/vpngateways. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkanalytics/dataproducts to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.networkanalytics/dataproducts. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkanalytics/dataproducts to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.networkanalytics/dataproducts. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkanalytics/dataproducts to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.networkanalytics/dataproducts. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkcloud/baremetalmachines to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.networkcloud/baremetalmachines. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkcloud/baremetalmachines to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.networkcloud/baremetalmachines. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkcloud/baremetalmachines to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.networkcloud/baremetalmachines. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkcloud/clusters to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.networkcloud/clusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category

group for microsoft.networkcloud/clusters to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.networkcloud/clusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkcloud/clusters to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.networkcloud/clusters. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkcloud/storageappliances to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.networkcloud/storageappliances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkcloud/storageappliances to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.networkcloud/storageappliances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkcloud/storageappliances to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.networkcloud/storageappliances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkfunction/azuretrafficcollectors to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.networkfunction/azuretrafficcollectors. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkfunction/azuretrafficcollectors to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.networkfunction/azuretrafficcollectors. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.networkfunction/azuretrafficcollectors to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.networkfunction/azuretrafficcollectors. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.notificationhubs/namespaces/notificationhubs to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.notificationhubs/namespaces/notificationhubs. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.notificationhubs/namespaces/notificationhubs to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics

workspace for microsoft.notificationhubs/namespaces/notificationhubs. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.notificationhubs/namespaces/notificationhubs to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.notificationhubs/namespaces/notificationhubs. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.openenergyplatform/energyservices to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.openenergyplatform/energyservices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.openenergyplatform/energyservices to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.openenergyplatform/energyservices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.openenergyplatform/energyservices to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.openenergyplatform/energyservices. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.powerbi/tenants/workspaces to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.powerbi/tenants/workspaces. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.powerbi/tenants/workspaces to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.powerbi/tenants/workspaces. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.powerbi/tenants/workspaces to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.powerbi/tenants/workspaces. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.servicenetworking/trafficcontrollers to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.servicenetworking/trafficcontrollers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.servicenetworking/trafficcontrollers to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.servicenetworking/trafficcontrollers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.servicenetworking/trafficcontrollers to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This

policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.servicenetworking/trafficcontrollers. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.synapse/workspaces/kustopools to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.synapse/workspaces/kustopools. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.synapse/workspaces/kustopools to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.synapse/workspaces/kustopools. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.synapse/workspaces/kustopools to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.synapse/workspaces/kustopools. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.timeseriesinsights/environments to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.timeseriesinsights/environments. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.timeseriesinsights/environments to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.timeseriesinsights/environments. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.timeseriesinsights/environments to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.timeseriesinsights/environments. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.timeseriesinsights/environments/eventsources to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.timeseriesinsights/environments/eventsources. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.timeseriesinsights/environments/eventsources to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.timeseriesinsights/environments/eventsources. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.timeseriesinsights/environments/eventsources to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.timeseriesinsights/environments/eventsources. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.workloads/sapvirtualinstances to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into

any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for microsoft.workloads/sapvirtualinstances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.workloads/sapvirtualinstances to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for microsoft.workloads/sapvirtualinstances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for microsoft.workloads/sapvirtualinstances to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for microsoft.workloads/sapvirtualinstances. DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Network Managers (microsoft.network/networkmanagers) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Network Managers (microsoft.network/networkmanagers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Network Managers (microsoft.network/networkmanagers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Network Managers (microsoft.network/networkmanagers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Network Managers (microsoft.network/networkmanagers) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Network Managers (microsoft.network/networkmanagers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Network security groups (microsoft.network/networksecuritygroups) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Network security groups (microsoft.network/networksecuritygroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Network security groups (microsoft.network/networksecuritygroups) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Network security groups (microsoft.network/networksecuritygroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Network security groups (microsoft.network/networksecuritygroups) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Network security groups (microsoft.network/networksecuritygroups). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Notification Hub Namespaces (microsoft.notificationhubs/namespaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Notification Hub Namespaces (microsoft.notificationhubs/namespaces). DeployIfNotExists, AuditIfNotExists,

Disabled 1.0.0 Enable logging by category group for Notification Hub Namespaces (microsoft.notificationhubs/namespaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Notification Hub Namespaces (microsoft.notificationhubs/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Notification Hub Namespaces (microsoft.notificationhubs/namespaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Notification Hub Namespaces (microsoft.notificationhubs/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Playwright Testing (microsoft.azureplaywrightservice/accounts) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Playwright Testing (microsoft.azureplaywrightservice/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Playwright Testing (microsoft.azureplaywrightservice/accounts) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Playwright Testing (microsoft.azureplaywrightservice/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Playwright Testing (microsoft.azureplaywrightservice/accounts) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Playwright Testing (microsoft.azureplaywrightservice/accounts). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for PostgreSQL flexible server (microsoft.dbforpostgresql/flexibleservers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Database for PostgreSQL flexible server (microsoft.dbforpostgresql/flexibleservers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Power BI Embedded (microsoft.powerbidedicated/capacities) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Power BI Embedded (microsoft.powerbidedicated/capacities). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Power BI Embedded (microsoft.powerbidedicated/capacities) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Power BI Embedded (microsoft.powerbidedicated/capacities). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Power BI Embedded (microsoft.powerbidedicated/capacities) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Power BI Embedded (microsoft.powerbidedicated/capacities). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by

category group for Public IP addresses (microsoft.network/publicipaddresses) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Public IP addresses (microsoft.network/publicipaddresses). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Public IP addresses (microsoft.network/publicipaddresses) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Public IP addresses (microsoft.network/publicipaddresses). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Public IP addresses (microsoft.network/publicipaddresses) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Public IP addresses (microsoft.network/publicipaddresses). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Public IP Prefixes (microsoft.network/publicipprefixes) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Public IP Prefixes (microsoft.network/publicipprefixes). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Public IP Prefixes (microsoft.network/publicipprefixes) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Public IP Prefixes (microsoft.network/publicipprefixes). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Public IP Prefixes (microsoft.network/publicipprefixes) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Public IP Prefixes (microsoft.network/publicipprefixes). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Recovery Services vaults (microsoft.recoveryservices/vaults) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Recovery Services vaults (microsoft.recoveryservices/vaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Recovery Services vaults (microsoft.recoveryservices/vaults) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Recovery Services vaults (microsoft.recoveryservices/vaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Recovery Services vaults (microsoft.recoveryservices/vaults) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Recovery Services vaults (microsoft.recoveryservices/vaults). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Relays (microsoft.relay/namespaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any

changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Relays (microsoft.relay/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Relays (microsoft.relay/namespaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Relays (microsoft.relay/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Relays (microsoft.relay/namespaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Relays (microsoft.relay/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Scaling plans (microsoft.desktopvirtualization/scalingplans) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Scaling plans (microsoft.desktopvirtualization/scalingplans). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Scaling plans (microsoft.desktopvirtualization/scalingplans) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Scaling plans (microsoft.desktopvirtualization/scalingplans). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Scaling plans (microsoft.desktopvirtualization/scalingplans) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Scaling plans (microsoft.desktopvirtualization/scalingplans). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for SCOPE pools (microsoft.synapse/workspaces/scopepools) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for SCOPE pools (microsoft.synapse/workspaces/scopepools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for SCOPE pools (microsoft.synapse/workspaces/scopepools) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for SCOPE pools (microsoft.synapse/workspaces/scopepools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for SCOPE pools (microsoft.synapse/workspaces/scopepools) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for SCOPE pools (microsoft.synapse/workspaces/scopepools). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Search services (microsoft.search/searchservices) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Search services (microsoft.search/searchservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Search services (microsoft.search/searchservices) to Log Analytics

Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Search services (microsoft.search/searchservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Search services (microsoft.search/searchservices) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Search services (microsoft.search/searchservices). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Service Bus Namespaces (microsoft.servicebus/namespaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Service Bus Namespaces (microsoft.servicebus/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Service Bus Namespaces (microsoft.servicebus/namespaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Service Bus Namespaces (microsoft.servicebus/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Service Bus Namespaces (microsoft.servicebus/namespaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Service Bus Namespaces (microsoft.servicebus/namespaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for SignalR (microsoft.signalrservice/signalr) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for SignalR (microsoft.signalrservice/signalr). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for SignalR (microsoft.signalrservice/signalr) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for SignalR (microsoft.signalrservice/signalr). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for SignalR (microsoft.signalrservice/signalr) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for SignalR (microsoft.signalrservice/signalr). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for SQL databases (microsoft.sql/servers/databases) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for SQL databases (microsoft.sql/servers/databases). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for SQL databases (microsoft.sql/servers/databases) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for SQL databases (microsoft.sql/servers/databases). DeployIfNotExists,

AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for SQL databases (microsoft.sql/servers/databases) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for SQL databases (microsoft.sql/servers/databases). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for SQL managed instances (microsoft.sql/managedinstances) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for SQL managed instances (microsoft.sql/managedinstances). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for SQL managed instances (microsoft.sql/managedinstances) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for SQL managed instances (microsoft.sql/managedinstances). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for SQL managed instances (microsoft.sql/managedinstances) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for SQL managed instances (microsoft.sql/managedinstances). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Storage movers (microsoft.storagemover/storagemovers) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Storage movers (microsoft.storagemover/storagemovers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Storage movers (microsoft.storagemover/storagemovers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Storage movers (microsoft.storagemover/storagemovers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Storage movers (microsoft.storagemover/storagemovers) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Storage movers (microsoft.storagemover/storagemovers). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Stream Analytics jobs (microsoft.streamanalytics/streamingjobs) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Stream Analytics jobs (microsoft.streamanalytics/streamingjobs). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Stream Analytics jobs (microsoft.streamanalytics/streamingjobs) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Stream Analytics jobs (microsoft.streamanalytics/streamingjobs). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Stream Analytics jobs (microsoft.streamanalytics/streamingjobs) to Storage Resource logs should be enabled to track activities and

events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Stream Analytics jobs (microsoft.streamanalytics/streamingjobs). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Streaming Endpoints (microsoft.media/mediaservices/streamingendpoints) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Streaming Endpoints (microsoft.media/mediaservices/streamingendpoints). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Streaming Endpoints (microsoft.media/mediaservices/streamingendpoints) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Streaming Endpoints (microsoft.media/mediaservices/streamingendpoints). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Streaming Endpoints (microsoft.media/mediaservices/streamingendpoints) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Streaming Endpoints (microsoft.media/mediaservices/streamingendpoints). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Traffic Manager profiles (microsoft.network/trafficmanagerprofiles) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Traffic Manager profiles (microsoft.network/trafficmanagerprofiles). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Traffic Manager profiles (microsoft.network/trafficmanagerprofiles) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Traffic Manager profiles (microsoft.network/trafficmanagerprofiles). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Traffic Manager profiles (microsoft.network/trafficmanagerprofiles) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Traffic Manager profiles (microsoft.network/trafficmanagerprofiles). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Video Analyzers (microsoft.media/videoanalyzers) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Video Analyzers (microsoft.media/videoanalyzers). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Video Analyzers (microsoft.media/videoanalyzers) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Video Analyzers (microsoft.media/videoanalyzers). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Video Analyzers (microsoft.media/videoanalyzers) to Storage Resource logs should be enabled to track activities and events that

take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Video Analyzers (microsoft.media/videoanalyzers). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Virtual network gateways (microsoft.network/virtualnetworkgateways) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Virtual network gateways (microsoft.network/virtualnetworkgateways). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Virtual network gateways (microsoft.network/virtualnetworkgateways) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Virtual network gateways (microsoft.network/virtualnetworkgateways). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Virtual network gateways (microsoft.network/virtualnetworkgateways) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Virtual network gateways (microsoft.network/virtualnetworkgateways). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Virtual networks (microsoft.network/virtualnetworks) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Virtual networks (microsoft.network/virtualnetworks). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Virtual networks (microsoft.network/virtualnetworks) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Virtual networks (microsoft.network/virtualnetworks). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Virtual networks (microsoft.network/virtualnetworks) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Virtual networks (microsoft.network/virtualnetworks). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Volumes (microsoft.netapp/netappaccounts/capacitypools/volumes) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Volumes (microsoft.netapp/netappaccounts/capacitypools/volumes). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Volumes (microsoft.netapp/netappaccounts/capacitypools/volumes) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Volumes (microsoft.netapp/netappaccounts/capacitypools/volumes). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Volumes (microsoft.netapp/netappaccounts/capacitypools/volumes) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give

you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Volumes (microsoft.netapp/netappaccounts/capacitypools/volumes). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Web PubSub Service (microsoft.signalrservice/webpubsub) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Web PubSub Service (microsoft.signalrservice/webpubsub). DeployIfNotExists, AuditIfNotExists, Disabled 1.2.0 Enable logging by category group for Web PubSub Service (microsoft.signalrservice/webpubsub) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Web PubSub Service (microsoft.signalrservice/webpubsub). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Web PubSub Service (microsoft.signalrservice/webpubsub) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Web PubSub Service (microsoft.signalrservice/webpubsub). DeployIfNotExists, AuditIfNotExists, Disabled 1.1.0 Enable logging by category group for Workspace (microsoft.desktopvirtualization/workspaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Azure Virtual Desktop Workspace (microsoft.desktopvirtualization/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Workspaces (microsoft.desktopvirtualization/workspaces) to Event Hub Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to an Event Hub for Workspaces (microsoft.desktopvirtualization/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Workspaces (microsoft.desktopvirtualization/workspaces) to Log Analytics Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Log Analytics workspace for Workspaces (microsoft.desktopvirtualization/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Enable logging by category group for Workspaces (microsoft.desktopvirtualization/workspaces) to Storage Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. This policy deploys a diagnostic setting using a category group to route logs to a Storage Account for Workspaces (microsoft.desktopvirtualization/workspaces). DeployIfNotExists, AuditIfNotExists, Disabled 1.0.0 Linux Arc-enabled machines should have Azure Monitor Agent installed Linux Arc-enabled machines should be monitored and secured through the deployed Azure Monitor Agent. The Azure Monitor Agent collects telemetry data from the guest OS. This policy will audit Arc-enabled machines in supported regions. Learn more: https://aka.ms/AMAOverview. AuditIfNotExists, Disabled 1.2.0 Linux virtual machine scale sets should have Azure Monitor Agent installed Linux virtual machine scale sets should be monitored and secured through the deployed Azure Monitor Agent. The Azure Monitor Agent collects telemetry data from the guest OS. This policy will audit virtual machine scale sets with supported OS images in supported regions. Learn more: https://aka.ms/AMAOverview. AuditIfNotExists, Disabled 3.6.0 Linux virtual machines should have Azure

Monitor Agent installed Linux virtual machines should be monitored and secured through the deployed Azure Monitor Agent. The Azure Monitor Agent collects telemetry data from the guest OS. This policy will audit virtual machines with supported OS images in supported regions. Learn more: https://aka.ms/AMAOverview. AuditIfNotExists, Disabled 3.6.0 Log Analytics workspaces should block log ingestion and querying from public networks Improve workspace security by blocking log ingestion and querying from public networks. Only private-link connected networks will be able to ingest and query logs on this workspace. Learn more at https://aka.ms/AzMonPrivateLink#configure-log-analytics. audit, Audit, deny, Deny, disabled, Disabled 1.1.0 Log Analytics Workspaces should block non-Azure Active Directory based ingestion. Enforcing log ingestion to require Azure Active Directory authentication prevents unauthenticated logs from an attacker which could lead to incorrect status, false alerts, and incorrect logs stored in the system. Deny, Audit, Disabled 1.0.0 Public IP addresses should have resource logs enabled for Azure DDoS Protection Enable resource logs for public IP addressess in diagnostic settings to stream to a Log Analytics workspace. Get detailed visibility into attack traffic and actions taken to mitigate DDoS attacks via notifications, reports and flow logs. AuditIfNotExists, DeployIfNotExists, Disabled 1.0.1 Resource logs should be enabled for Audit on supported resources Resource logs should be enabled to track activities and events that take place on your resources and give you visibility and insights into any changes that occur. The existence of a diagnostic setting for category group Audit on the selected resource types ensures that these logs are enabled and captured. Applicable resource types are those that support the "Audit" category group. AuditIfNotExists, Disabled 1.0.0 Saved-queries in Azure Monitor should be saved in customer storage account for logs encryption Link storage account to Log Analytics workspace to protect saved-queries with storage account encryption. Customer-managed keys are commonly required to meet regulatory compliance and for more control over the access to your saved-queries in Azure Monitor. For more details on the above, see https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys?tabs=portal#customer-managed-key-for-saved-queries. audit, Audit, deny, Deny, disabled, Disabled 1.1.0 Storage account containing the container with activity logs must be encrypted with BYOK This policy audits if the Storage account containing the container with activity logs is encrypted with BYOK. The policy works only if the storage account lies on the same subscription as activity logs by design. More information on Azure Storage encryption at rest can be found here https://aka.ms/azurestoragebyok. AuditIfNotExists, Disabled 1.0.0 The legacy Log Analytics extension should not be installed on Azure Arc enabled Linux servers Automatically prevent installation of the legacy Log Analytics Agent as the final step of migrating from legacy agents to Azure Monitor Agent. After you have uninstalled existing legacy extensions, this policy will deny all future installations of the legacy agent extension on Azure Arc enabled Linux servers. Learn more: https://aka.ms/migratetoAMA Deny, Audit, Disabled 1.0.0 The legacy Log Analytics extension should not be installed on Azure Arc enabled Windows servers Automatically prevent installation of the legacy Log Analytics Agent as the final step of migrating from legacy agents to Azure Monitor Agent. After you have uninstalled existing legacy extensions, this policy will deny all future installations of the legacy agent extension on Azure Arc enabled Windows servers. Learn more: https://aka.ms/migratetoAMA Deny, Audit, Disabled 1.0.0 The legacy Log Analytics extension should not be installed on Linux virtual machine scale sets Automatically prevent installation of the legacy Log Analytics Agent as the final step of migrating from legacy agents to Azure Monitor Agent. After you have uninstalled existing legacy extensions, this policy will deny all future installations of the legacy agent extension on Linux virtual machine scale sets. Learn more: https://aka.ms/migratetoAMA Deny, Audit, Disabled 1.0.0 The legacy Log Analytics extension should not be installed on Linux virtual machines Automatically prevent installation of the legacy Log Analytics Agent as the final step of migrating from legacy agents to Azure Monitor Agent. After you

have uninstalled existing legacy extensions, this policy will deny all future installations of the legacy agent extension on Linux virtual machines. Learn more: https://aka.ms/migratetoAMA Deny, Audit, Disabled 1.0.0 The legacy Log Analytics extension should not be installed on virtual machine scale sets Automatically prevent installation of the legacy Log Analytics Agent as the final step of migrating from legacy agents to Azure Monitor Agent. After you have uninstalled existing legacy extensions, this policy will deny all future installations of the legacy agent extension on Windows virtual machine scale sets. Learn more: https://aka.ms/migratetoAMA Deny, Audit, Disabled 1.0.0 The legacy Log Analytics extension should not be installed on virtual machines Automatically prevent installation of the legacy Log Analytics Agent as the final step of migrating from legacy agents to Azure Monitor Agent. After you have uninstalled existing legacy extensions, this policy will deny all future installations of the legacy agent extension on Windows virtual machines. Learn more: https://aka.ms/migratetoAMA Deny, Audit, Disabled 1.0.0 Windows Arc-enabled machines should have Azure Monitor Agent installed Windows Arc-enabled machines should be monitored and secured through the deployed Azure Monitor Agent. The Azure Monitor Agent collects telemetry data from the guest OS. Windows Arc-enabled machines in supported regions are monitored for Azure Monitor Agent deployment. Learn more: https://aka.ms/AMAOverview. AuditIfNotExists, Disabled 1.4.0 Windows virtual machine scale sets should have Azure Monitor Agent installed Windows virtual machine scale sets should be monitored and secured through the deployed Azure Monitor Agent. The Azure Monitor Agent collects telemetry data from the guest OS. Virtual machine scale sets with supported OS and in supported regions are monitored for Azure Monitor Agent deployment. Learn more: https://aka.ms/AMAOverview. AuditIfNotExists, Disabled 3.5.0 Windows virtual machines should have Azure Monitor Agent installed Windows virtual machines should be monitored and secured through the deployed Azure Monitor Agent. The Azure Monitor Agent collects telemetry data from the guest OS. Windows virtual machines with supported OS and in supported regions are monitored for Azure Monitor Agent deployment. Learn more: https://aka.ms/AMAOverview. AuditIfNotExists, Disabled 3.5.0 Workbooks should be saved to storage accounts that you control With bring your own storage (BYOS), your workbooks are uploaded into a storage account that you control. That means you control the encryption-at-rest policy, the lifetime management policy, and network access. You will, however, be responsible for the costs associated with that storage account. For more information, visit https://aka.ms/workbooksByos deny, Deny, audit, Audit, disabled, Disabled 1.1.0
