AZURE OPERATIONAL SECURITY

September 2018

Disclaimer

This document is for informational purposes only. MICROSOFT MAKE NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided “as-is.” Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

NOTE: Certain recommendations in this white paper may result in increased data, network, or compute resource usage, and may increase your license or subscription costs.

Executive summary

Microsoft Azure operational security refers to the services, controls, and features available to users for protecting their data, applications, and other assets in Azure. Azure operational security is built on a framework that incorporates the knowledge gained through various capabilities that are unique to Microsoft, including the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape.

This white paper outlines how you can approach operational security by using Azure. It covers several Azure services.

Contents

Overview

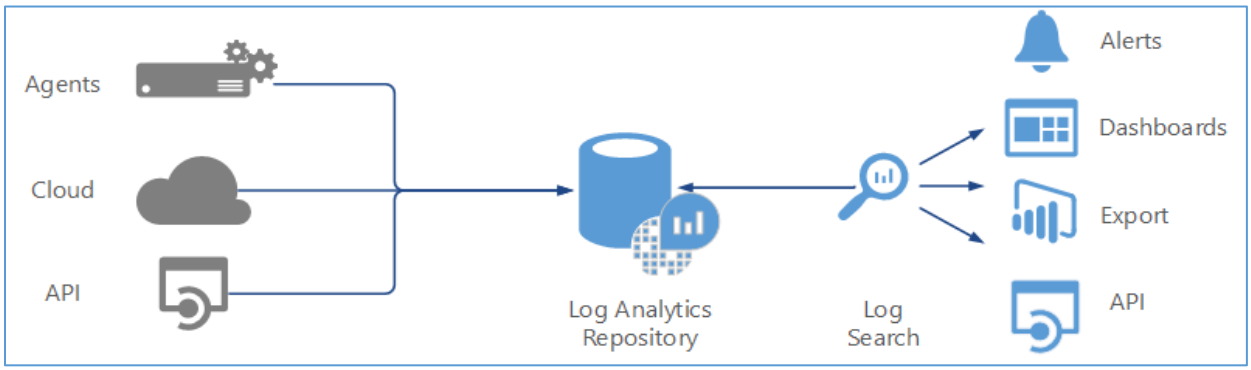
Security is paramount in the cloud. The tools and capabilities in Microsoft Azure can help you create secure solutions on the Azure platform.

Azure provides confidentiality, integrity, and availability of customer data, while also enabling transparent accountability. This paper describes the Azure services that you can use to enhance operational security.

Azure Log Analytics

Azure Log Analytics plays a central role in Azure management by collecting telemetry and other data from a variety of sources. It provides a query language and analytics engine that gives you insights into the operation of your applications and resources. You can interact directly with Log Analytics data through log searches and views. Or you can use analysis tools in other Azure services that store their data in Log Analytics, such as Azure Application Insights or Azure Security Center.

As shown in the following diagram, Log Analytics enables you to consolidate data from various sources, so you can combine data from your Azure services with your existing on-premises environment. It also clearly separates the collection of the data from the action taken on that data, so that all actions are available to all kinds of data.



Log Analytics manages your cloud-based data securely by using the following methods:

- Data segregation
- Data retention
- Physical security
- Incident management
- Compliance
- Security standards certifications

Log Analytics includes an interactive and expressive query language, machine learning constructs, and a portal for advanced analytics. The portal offers a multiline query editor, full schema view, and rich visualizations to help you get deeper insights from your data.

Your Log Analytics workspace can take advantage of the following language benefits:

- Simple yet powerful: Similar to SQL with constructs like a natural language.
- Full piping language: Extensive piping capabilities where any output can be piped to another command to create complex queries.
- Search-time field extractions: Calculated fields at runtime so you can use complex calculations for extended fields and then use them for additional commands, including joins and aggregations.
- Advanced joins: Ability to join tables on multiple fields, using inner and outer joins, and join on extended fields.
- Date/time functions: Advanced date/time functions that give you flexibility.
- Smart Analytics: Advanced algorithms to evaluate patterns in datasets and compare different sets of data.

Azure Backup

You can use Azure Backup to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that's reliable, secure, and cost-competitive. Azure Backup offers multiple components that you download and deploy on the appropriate computer or server, or in the cloud. The component, or agent, that you deploy depends on what you want to protect. All Azure Backup components (whether you're protecting data on-premises or in the cloud) can be used to back up data to an Azure Site Recovery vault.

The backup vault is located in a particular geographic region. The data is replicated within the same region. Depending on the type of vault, the data might also be replicated to another region for further resiliency.

Management solutions

Management solutions take advantage of services in Azure to provide additional insight into the operation of a particular application or service. Management solutions typically collect information in Log Analytics and provide log searches and views to analyze collected data. They might also use other services, such as Azure Automation, to perform actions related to the application or service.

You can add management solutions to your Azure subscription for any applications and services that you use. They're typically available at no cost, but they collect data that might invoke usage charges. In addition to solutions provided by Microsoft, partners and customers can create management solutions to use them in their own environment or to make them available to customers through the community.

A good example of a solution that uses multiple services to provide additional functionality is Update Management. This solution uses the Log Analytics agent for Windows and Linux to collect information about required updates on each agent. It writes this data to the Log Analytics repository, where you can analyze it by using an included dashboard.

When you create a deployment, runbooks in Azure Automation are used to install required updates. You manage this entire process in the portal, and you don't need to worry about the underlying details.

Azure Security Center

Azure Security Center uses advanced analytics and global threat intelligence to detect incoming attacks and post-breach activity. Alerts are prioritized and grouped into incidents, helping you focus on the most critical threats first. Security Center analyzes the security state of your Azure and non-Azure resources to identify potential security vulnerabilities.

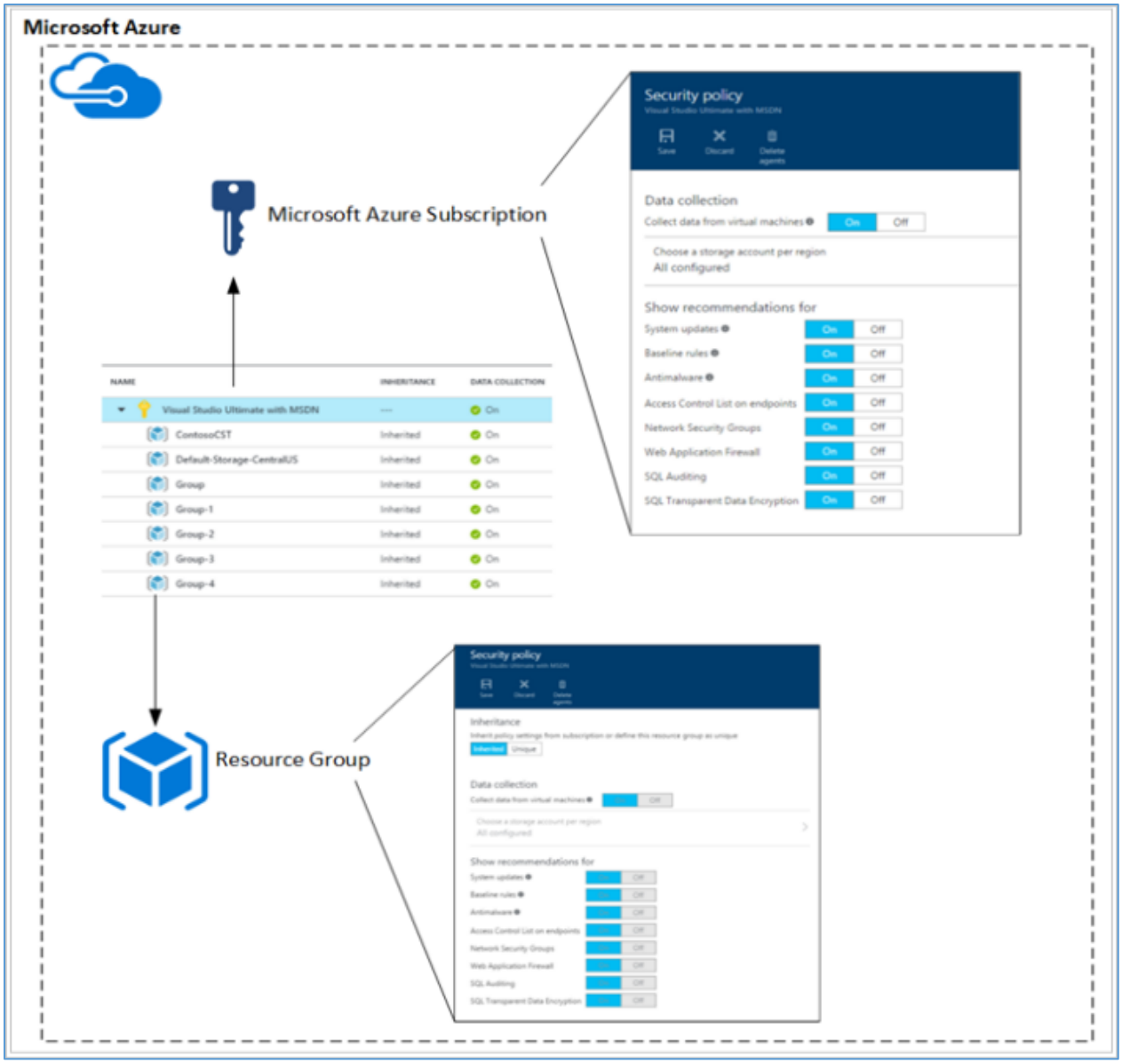
Azure Security Center provides integrated security monitoring and policy management across your Azure subscriptions. You can define polices not only against your Azure subscriptions, but also against resource groups so you can be more detailed.

Azure Security Center helps you protect workloads running in Azure, running on-premises, and running in other clouds. Managing security across an increasingly distributed infrastructure is complex and can create gaps that attackers exploit. Security Center reduces this complexity by unifying security management across environments and providing intelligent threat protection by using analytics and the Microsoft Intelligent Security Graph.

Security policies and recommendations

A security policy defines the controls that are recommended for resources within the specified subscription or resource group. In Security Center, you define policies according to your company's security requirements, the type of applications, and the sensitivity of the data.

Policies that you enable in the subscription level automatically propagate to all resource groups within the subscription, as shown in this diagram:



Data collection

Security Center collects data from your virtual machines (VMs) to assess their security state, provide security recommendations, and alert you to threats. When you first access Security Center, data collection is enabled on all VMs in your subscription. We recommend data collection, but you can opt out by turning off data collection in the Security Center policy.

Data sources

Azure Security Center analyzes data from the following sources to provide visibility into your security state, identify vulnerabilities and recommend mitigations, and detect active threats:

- **Azure services**: Uses information about the configuration of Azure services you have deployed by communicating with the resource providers for those services.

- **Network traffic**: Uses sampled network traffic metadata from the Microsoft infrastructure, such as source/destination IP/port, packet size, and network protocol.
- **Partner solutions**: Uses security alerts from integrated partner solutions, such as firewalls and antimalware solutions.
- **Your virtual machines**: Uses configuration information and information about security events, such as Windows event and audit logs, IIS logs, Syslog messages, and crash dump files from your virtual machines.

Data protection

To help you prevent, detect, and respond to threats, Azure Security Center collects and processes security-related data. This data includes configuration information, metadata, and event logs. Microsoft adheres to strict compliance and security guidelines—from coding to operating a service.

- Data segregation: Data is kept logically separate on each component throughout the service. All data is tagged per organization. This tagging persists throughout the data lifecycle, and it's enforced at each layer of the service.
- **Data access**: To provide security recommendations and investigate potential security threats, Microsoft personnel might access information collected or analyzed by Azure services, including crash dump files, process creation events, VM disk snapshots, and artifacts. This information might unintentionally include customer data or personal data from your virtual machines. We adhere to the Microsoft Software License Terms, which states that Microsoft won't use customer data, or derive information from it, for any advertising or similar commercial purposes.
- **Data use**: Microsoft uses patterns and threat intelligence viewed across multiple tenants to enhance its prevention and detection capabilities. It does so in accordance with the privacy commitments described in the Microsoft Trust Center.

Data location

Azure Security Center collects ephemeral copies of your crash dump files and analyzes them for evidence of exploit attempts and successful compromises. Azure Security Center performs this analysis within the same geo as the workspace, and it deletes the ephemeral copies when analysis is complete. Machine artifacts are stored centrally in the same region as the VM.

A storage account is specified for each region where virtual machines are running. So you can to store data in the same region as the virtual machine from which the data is collected.

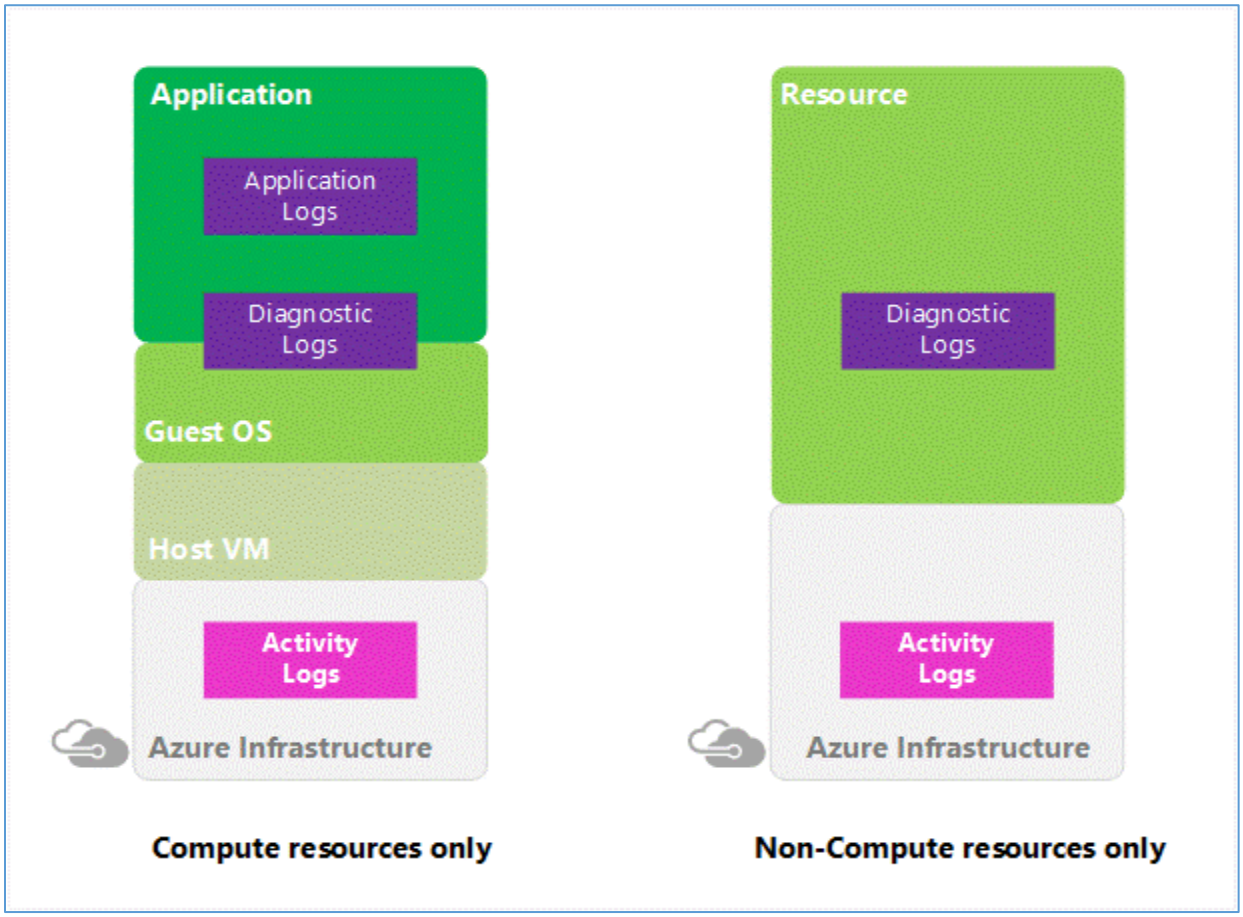
Information about security alerts—including partner alerts, recommendations, and security health status—is stored centrally, currently in the United States. This information might include related configuration information and security events collected from your virtual machines as needed to provide you with the security alert, recommendation, or security health status.

Azure Monitor

Azure Monitor provides base-level infrastructure metrics and logs for most services in Microsoft Azure.

Microsoft offers additional products and services that provide monitoring capabilities for developers, DevOps, or IT Ops that also have on-premises installations. For an overview and understanding of how these products and services work together, see Monitoring in Microsoft Azure.

The following diagram is an overview of the logging components of Azure Monitor:



Azure Activity Log

The Azure Activity Log provides insight into the operations that were performed on resources in your subscription. This log was previously known as Audit Logs or Operational Logs, because it reports control-plane events for your subscriptions.

Categories in the Activity Log include:

- **Administrative**: This category contains the record of all create, update, delete, and action operations performed through Azure Resource Manager. Examples of event types in this category include "create virtual machine" and "delete network security group." Every action that a user or application takes by using Resource Manager is modeled as an operation on a resource type. If the operation type is Write, Delete, or Action, the records of both the start and success or failure of that operation are recorded in the Administrative category. The Administrative category also includes any changes to role-based access control in a subscription.

- **Service Health**: This category contains the record of any service health incidents that have occurred in Azure. An example of an event type in this category is "SQL Azure in East US is experiencing downtime." Service health events come in five varieties: Action Required, Assisted Recovery, Incident, Maintenance, Information, or Security. They appear only if you have a resource in the subscription that the event would affect.
- **Alert**: This category contains the record of all activations of Azure alerts. An example of an event type in this category is "CPU % on my VM has been over 80 for the past 5 minutes." A variety of Azure systems have an alerting concept—you can define a rule of some sort and receive a notification when conditions match that rule. Each time a supported Azure alert type is activated, or the conditions are met to generate a notification, a record of the activation is also pushed to this category of the Activity Log.
- **Autoscale**: This category contains the record of any events related to the operation of the autoscale engine based on any autoscale settings you've defined in your subscription. An example of an event type in this category is "Autoscale scale up action failed." By using an autoscale setting, you can automatically scale out or scale in the number of instances in a supported resource type based on time of day and/or load (metric) data. When the conditions are met to scale up or down, the started and succeeded or failed events are recorded in this category.
- **Recommendation**: This category contains recommendation events from certain resource types, such as websites and SQL servers. These events offer recommendations for how to better utilize your resources. You receive events of this type only if you have resources that emit recommendations.
- **Security**: This category contains the record of any alerts that Azure Security Center generates. An example of an event type in this category is "Suspicious double extension file executed."
- **Policy and Resource Health**: These categories don't contain any events. They're reserved for future use.

By using the Activity Log, you can determine the "what, who, and when" for any write operations (PUT, POST, DELETE) taken on the resources in your subscription. You can also understand the status of the operation and other relevant properties. The Activity Log does not include read (GET) operations or operations for resources that use the classic model.

Azure diagnostic logs

Diagnostic logs are emitted by a resource and provide rich, frequent data about the operation of that resource. The content of these logs varies by resource type.

For example, Windows event system logs are one category of diagnostic log for VMs. Blob, table, and queue logs are categories of diagnostic logs for storage accounts.

Diagnostic logs differ from the Activity Log. The Activity Log provides insight into the operations that were performed on resources in your subscription. Diagnostic logs provide insight into operations that your resource performed itself.

Resource-level diagnostic logs also differ from guest OS-level diagnostic logs. Guest OS diagnostic logs are collected by an agent running inside a virtual machine or another supported resource type. Resource-level diagnostic logs require no agent and capture resource-specific data from the Azure

platform itself, whereas guest OS-level diagnostic logs capture data from the operating system and applications running on a virtual machine.

Azure Monitor routes your Azure resource diagnostic logs and metrics to storage accounts, Azure Event Hubs namespaces, or Log Analytics workspaces. You can create multiple resource diagnostic settings for each resource. Then you an route different permutations of log categories and metrics to different destinations (in public preview), and route your metrics and logs to a destination in a different subscription.

Metrics

Azure Monitor enables you to consume telemetry to gain visibility into the performance and health of your workloads on Azure. The most important type of Azure telemetry data is the metrics (also called performance counters) emitted by most Azure resources. Azure Monitor provides several ways to configure and consume these metrics for monitoring and troubleshooting. Metrics are a valuable source of telemetry and enable you to do the following tasks:

- Track the performance of your resource (such as a VM, website, or logic app) by plotting its metrics on a portal chart and pinning that chart to a dashboard.
- Get notified of an issue that affects the performance of your resource when a metric crosses a certain threshold.
- Configure automated actions, such as autoscaling a resource or firing a runbook when a metric crosses a certain threshold.
- Perform advanced analytics or reporting on performance or usage trends of your resource.
- Archive the performance or health history of your resource for compliance or auditing purposes.

Azure Monitor provides near real-time metric alerts in public preview for platform metrics from Azure services such as Azure Virtual Machines, Service Bus, and Event Hubs. Azure Monitor also enables new metrics and logs to be surfaced from many services, such as Azure Storage, Traffic Manager, Virtual Network, ExpressRoute, Load Balancer, Data Lake Store, and Data Lake Analytics. Near real-time metric alerts provide the following benefits:

- **Low latency**: You can create near real-time metric alerts that monitor metric values as frequently as 1 minute.
- **Control over metric conditions**: You can create near real-time metric alert rules that can monitor minimum, maximum, average, and total of the metric over the evaluation period.
- **Combined monitoring of multiple metrics**: You can create a single near real-time metric alert rule that can monitor multiple metrics (currently two) at the same time.
- **Modular notification system**: You can use action groups with near real-time metric alerts. Action groups provide a reusable set of actions for multiple alerts. By using action groups with near real-time metric alerts, you can send SMS, send email, or call a webhook when an alert is triggered.

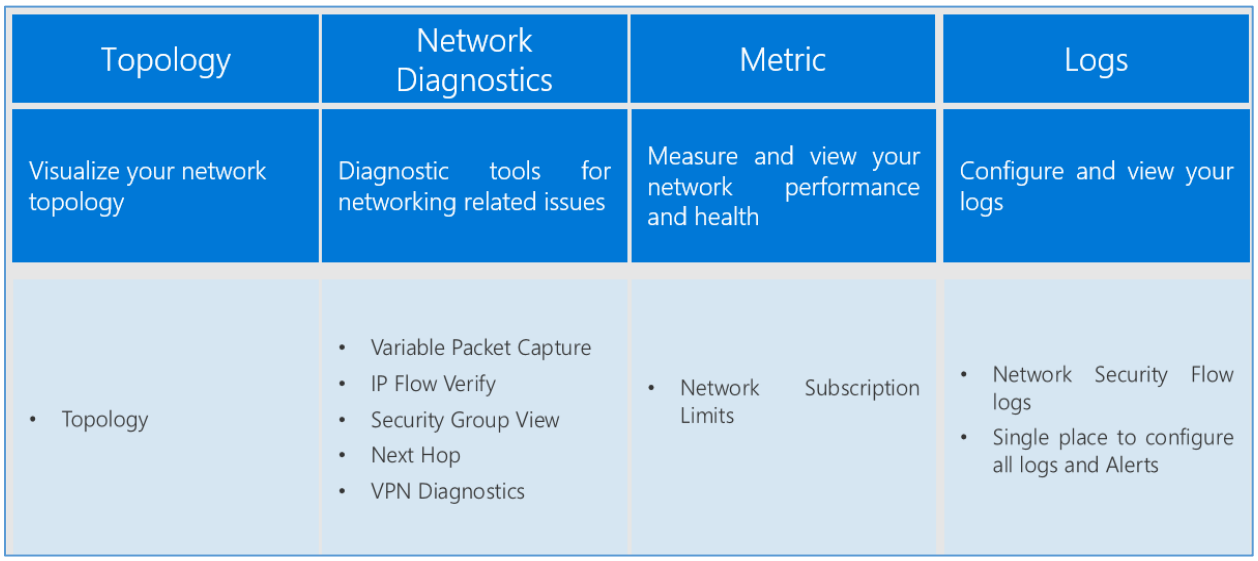
Azure Diagnostics

Azure Diagnostics enables the collection of diagnostic data on a deployed application. You can use the diagnostics extension from various different sources. Currently supported are Azure Cloud Services web

and worker roles, Azure Virtual Machines running Microsoft Windows, and Azure Service Fabric. Other Azure services have their own separate diagnostics.

Azure Network Watcher

Azure Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network level in, to, and from Azure. Scenario-level monitoring provides an end-to-end view of network resources, in contrast to individual network resource monitoring. The following figure outlines the features in Network Watcher:

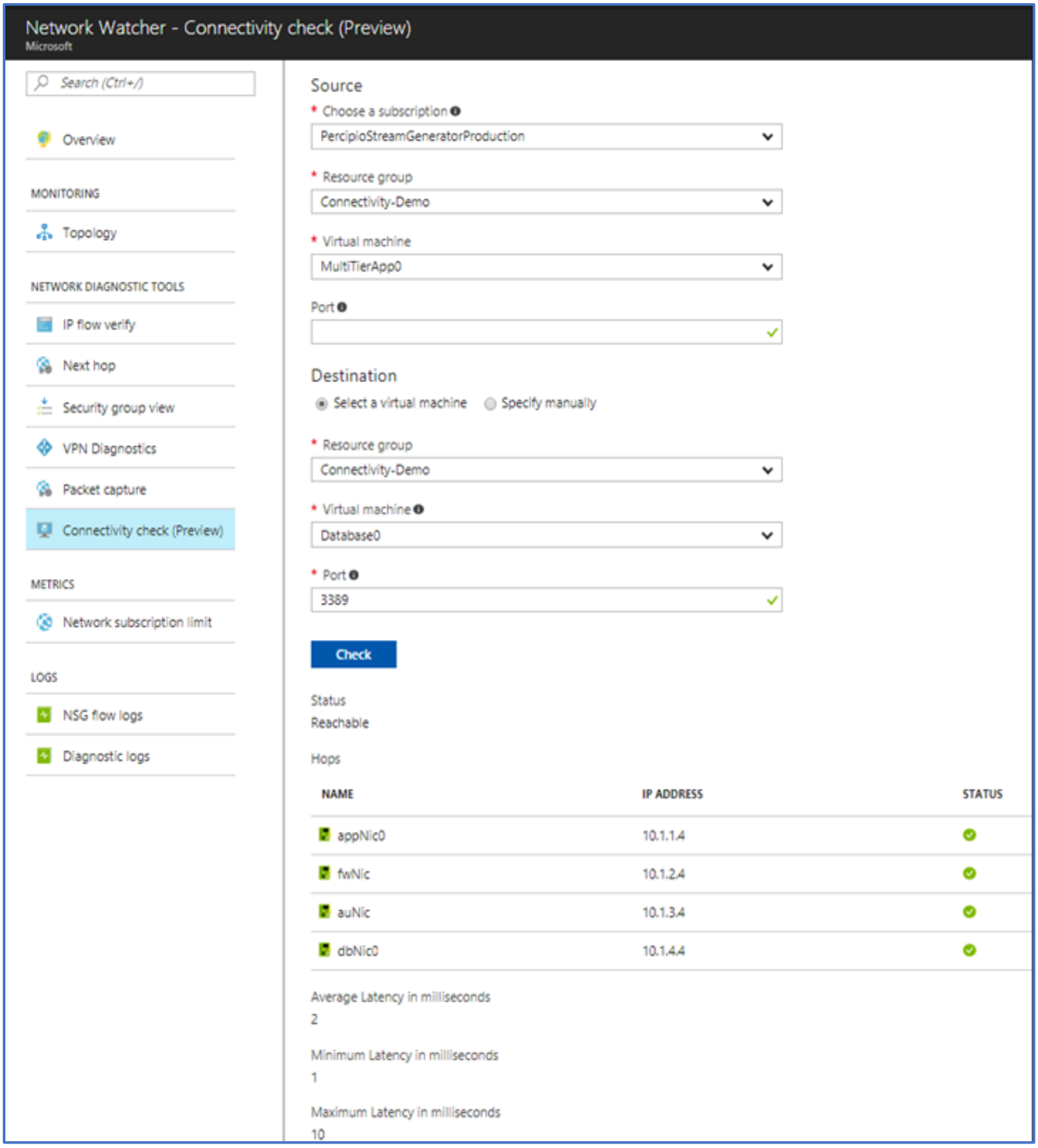


Network Watcher currently has the following capabilities:

- Network log: Logs operations performed as part of the configuration of networks. You can view these logs through the Azure portal, PowerShell, the Azure CLI, and the REST API. Or you can get them by using Microsoft tools (such as Power BI) or partner tools. For more information on audit logs, see Audit operations with Resource Manager. Audit logs are available for operations done on all network resources.
- IP flow verify: Checks if a packet is allowed or denied based on flow information 5-tuple packet parameters (destination IP, source IP, destination port, source port, and protocol). If a network security group denies the packet, the rule and network security group that denied the packet are returned.
- Next hop: Determines the next hop for packets being routed in the Azure network fabric, so you can diagnose any misconfigured user-defined routes.
- Security group view: Gets the effective and applied security rules on a VM. Auditing your network security is vital for detecting network vulnerabilities and ensuring compliance with your IT security and regulatory governance model. Security group view helps you determine which ports are open and assess network vulnerability.
- NSG flow log: Enables you to capture logs related to traffic that's allowed or denied by the security rules in a network security group. The flow is defined by 5-tuple information—destination IP, source IP, destination port, source port, and protocol.

- Connectivity check: Helps you quickly find and detect connectivity problems in the infrastructure, even as your network evolves in complexity. The returned results can provide valuable insights into whether a connectivity problem is due to a platform or a potential user configuration.

The following screenshot illustrates connectivity check:



You can use connectivity check from the Azure portal by using PowerShell, the Azure CLI, and the REST API.

Azure Storage Analytics

Azure Storage Analytics can store metrics that include aggregated transaction statistics and capacity data about requests to a storage service. Transactions are reported at both the API operation level and the storage service level, and capacity is reported at the storage service level. You can use metrics data to analyze storage service usage, diagnose problems with requests made against the storage service, and improve the performance of applications that use a service.

Storage Analytics performs logging and provides metrics data for a storage account. You can use this data to trace requests, analyze usage trends, and diagnose issues with your storage account. Storage Analytics logging is available for Azure Blob, Queue, and Table storage. Storage Analytics logs detailed information about successful and failed requests to a storage service.

Requests are logged on a best-effort basis. Log entries are created only if there are requests made against the service endpoint. For example, if a storage account has activity in its blob endpoint but not in its table or queue endpoint, only logs that pertain to the Blob service are created.

To use Storage Analytics, you must enable it individually for each service that you want to monitor. You can enable it in the Azure portal; for details, see Monitor a storage account in the Azure portal. You can also enable Storage Analytics programmatically via the REST API or the client library. Use the Set Service Properties operation to enable Storage Analytics individually for each service.

The aggregated data is stored in a well-known blob (for logging) and in well-known tables (for metrics). You can access the data by using the Blob service and Table service APIs.

Storage Analytics has a 20-TB limit on the amount of stored data that is independent of the total limit for your storage account. All logs are stored in block blobs in a container named $logs. The container is automatically created when Storage Analytics is enabled for a storage account.

The following actions performed by Storage Analytics are billable:

- Requests to create blobs for logging
- Requests to create table entities for metrics

Note: For more information on billing and data retention policies, see Storage Analytics and billing. For optimal performance, limit the number of highly utilized disks attached to the virtual machine to avoid possible throttling. If all disks are not being highly utilized at the same time, the storage account can support a larger number of disks.

For more information on storage account limits, see Azure Storage Scalability and Performance Targets.

Storage Analytics logs the following types of authenticated and anonymous requests:

Authenticated	Anonymous
Successful requests.	Successful requests.
Failed requests, including timeout, throttling, network, authorization, and other errors.	Requests that use a shared access signature, including failed and successful requests.
Requests that use a shared access signature, including failed and successful requests.	Time-out errors for both client and server.
Requests to analytics data.	Failed GET requests with error code 304 (Not Modified).
Requests made by Storage Analytics itself, such as log creation or deletion, are not logged. A full list of the logged data is documented in Storage Analytics Logged Operations and Status Messages and Storage Analytics Log Format.	All other failed anonymous requests are not logged. A full list of the logged data is documented in Storage Analytics Logged Operations and Status Messages and Storage Analytics Log Format.

Azure Active Directory

Azure Active Directory (Azure AD) includes a full suite of identity management capabilities. These capabilities include multi-factor authentication, device registration, self-service password management, self-service group management, privileged account management, role-based access control, application usage monitoring, rich auditing, and security monitoring and alerting.

Azure AD includes security, activity, and audit reports. Audit reports help you identify privileged actions that occurred in your Azure AD instance. Privileged actions include elevation changes (for example, role creation or password resets), changes to policy configurations (for example password policies), or changes to directory configuration (for example, changes to domain federation settings).

The reports provide the audit record for the event name, the actor who performed the action, the target resource affected by the change, and the date and time (in UTC). You can get the list of audit events for Azure AD via the Azure portal, as described in View your audit logs. Here's a list of the included reports:

Security reports	Activity reports	Audit reports
Sign-ins from unknown sources	Application usage: summary	Directory audit report
Sign-ins after multiple failures	Application usage: detailed	
Sign-ins from multiple geographies	Application dashboard	
Sign-ins from IP addresses with suspicious activity	Account provisioning errors	
Irregular sign-in activity	Individual user devices	
Sign-ins from possibly infected devices	Individual user activity	
Users with anomalous sign-in activity	Groups activity report	
	Password reset registration activity report	
	Password reset activity	

The data of these reports can be useful to your applications, such as SIEM systems, audit tools, and business intelligence tools. The Azure AD reporting APIs provide programmatic access to the data through a set of REST-based APIs. You can call these APIs from various programming languages and tools.

Azure AD retains events in audit reports for 180 days. For more information, see Azure Active Directory Report Retention Policies. If you're interested in storing audit events for longer retention periods, you can use the Reporting API to regularly pull audit events into a separate data store.

Azure AD is built to work for apps in the cloud, on mobile or on-premises. You can layer security features such as conditional access to help protect users and your business. Azure AD is also highly reliable. If a datacenter goes down, copies of your directory data are live in at least two more regionally dispersed datacenters and available for instant access.

Summary

This article summarizes ways you can protect your privacy and secure your data, while delivering software and services that help you manage the IT infrastructure of your organization. Microsoft

adheres to strict compliance and security guidelines—from coding to operating a service. Securing and protecting data is a top priority at Microsoft.

This article covered how to:

- Use Log Analytics to collect, process, and secure data.
- Quickly analyze events across multiple data sources. Identify security risks and understand the scope and impact of threats and attacks to mitigate the damage of a security breach.
- Identify attack patterns by visualizing outbound malicious IP traffic and malicious threat types. Understand the security posture of your entire environment regardless of platform.
- Capture all the log and event data required for a security or compliance audit. Reduce the time and resources needed to supply a security audit with a complete, searchable, and exportable log and event dataset.

Next steps

- Design and operational security: Learn how Microsoft designs its services and software with security in mind to help ensure that its cloud infrastructure is resilient and defended from attacks.
- Azure Security Center planning and operations: Follow a set of steps and tasks to optimize your use of Security Center based on your organization's security requirements and cloud management model.

Resources

GitHub repositories

- Azure Diagnostics Tools
- Audit Network Watcher Existence
- Troubleshoot connections with Azure Network Watcher using the Azure CLI 2.0

Samples

- Azure Resource Manager templates for Azure Backup
- Azure Monitor PowerShell quickstart samples

