Table of Contents

What is Operations Management Suite (OMS)?

2/16/2017 • 14 min to read • Edit Online

This article provides an introduction to Operations Management Suite (OMS) including a brief overview of the business value it provides, the services and management solutions it includes, and the offerings that package together different services and solutions. Links are included to the detailed documentation on deploying and using each service and solution.

From on-premise to the cloud

Microsoft has long been providing products for managing enterprise environments. Multiple products were consolidated into the System Center suite of management products in 2007. This included Configuration Manager which provides such features as software distribution and inventory, Operations Manager which provides proactive monitoring of systems and applications, Orchestrator which includes runbooks to automate manual processes, and Data Protection Manager for backup and recovery of critical data.

With more computing resources moving to the cloud, System Center products gained more cloud features such as Operations Manager and Orchestrator managing resources in Azure. They were still fundamentally designed as on-premise solutions though and require a significant investment in deploying and maintaining on-premise management environment. To completely leverage the cloud and support future applications, a new approach to management was required.

Introducing Operations Management Suite

Operations Management Suite (also known as OMS) is a collection of management services that were designed in the cloud from the start. Rather than deploying and managing on-premise resources, OMS components are entirely hosted in Azure. Configuration is minimal, and you can be up and running literally in a matter of minutes.

- **Minimal cost and complexity of deployment.** Because all of the components and data for OMS are stored in Azure, you can be up and running in a short time without the complexity and investment in on-premise components.
- **Scale to cloud levels.** You don't have to worry about paying for compute resources that you don't need or about running out of storage space since the cloud allows you to pay only for what you actually use and will readily scale to any load you require. You can start by managing a few resources to get started and then scale up to your entire environment.
- **Take advantage of the latest features.** Features in OMS services are continuously being added and updated. You constantly have access to the latest features without any requirement to deploy updates.
- **Integrated services.** While each of the OMS services provide significant value on their own, they can work together to solve complex management scenarios. For example, a runbook in Azure Automation might drive a failover process with Azure Site Recovery and then log information to Log Analytics to generate an alert.
- **Global knowledge.** Management solutions in OMS continuously have access to the latest information. The Security and Audit solution for example, can perform a threat analysis using the latest threats being detected around the world.
- **Access from anywhere.** Access your management environment from anywhere you have a browser. Install the OMS app on your smartphone for ready access to your monitoring data.

Is it just for the cloud?

Just because OMS services run in the cloud doesn't mean that they can't effectively manage your on-premise environment. Put an agent on any Windows or Linux computer in your data center, and it will send data to Log

Analytics where it can be analyzed along with all other data collected from cloud or on-premise services. Use Azure Backup and Azure Site Recovery to leverage the cloud for backup and high availability for on-premise resources.

Runbooks in the cloud can't typically access your on-premise resources, but you can install an agent on one or more computers too that will host runbooks in your data center. When you start a runbook, you simply specify whether you want it to run in the cloud or on a local worker.

Hybrid management with System Center

If you have an existing installation of System Center, you can integrate these components with OMS services to provide a hybrid solution for both your on-premise and cloud environments leveraging the relative specialties of each product. Connect your existing Operations Manager management group to Log Analytics to analyze managed agents in the cloud. Use your existing backup process with Data Protection Manager to backup your data to the cloud.

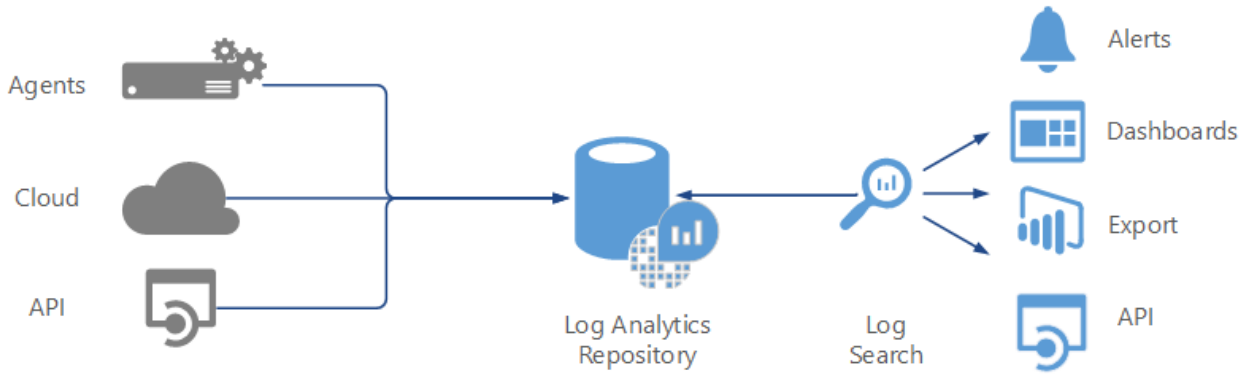
OMS services

The core functionality of OMS is provided by a set of services that run in Azure. Each service provides a specific management function, and you can combine services to achieve different management scenarios.

	SERVICE	DESCRIPTION
	Log Analytics	Monitor and analyze the availability and performance of different resources including physical and virtual machines.
	Automation	Automate manual processes and enforce configurations for physical and virtual machines.
	Backup	Backup and restore critical data.
	Site Recovery	Provide high availability for critical applications.

Log Analytics

Log Analytics provides monitoring services for OMS by collecting data from managed resources into a central repository. This data could include events, performance data, or custom data provided through the API. Once collected, the data is available for alerting, analysis, and export. This method allows you to consolidate data from a variety of sources so you can combine data from your Azure services with your existing on-premise 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.



Collecting data

There are a variety of ways that you can get data into the repository for Log Analytics to analyze.

- **Windows or Linux computers and virtual machines.** You install the Microsoft Monitoring Agent on Windows and Linux computers or virtual machines that you want to collect data from. The agent will automatically download from Log Analytics configuration that defines events and performance data to collect. You can easily install the agent on virtual machines running in Azure using the Azure portal. If you have an existing Operations Manager environment, you can connect the management group to Log Analytics and automatically start collecting data from all existing agents.
- **Azure services.** Log Analytics collects telemetry from Azure Diagnostics and Azure Monitoring into the repository so that you can monitor Azure resources.
- **Data Collector API.** Log Analytics has a REST API for populating data from any client. This allows you to collect data from third party applications or implement custom management scenarios. A common method is to use a runbook in Azure Automation to collect data and then use the Data Collector API to write it to the repository.

Reporting and analyzing data

Log Analytics includes a powerful query language to extract data stored in the repository. Since data from all sources are stored as records, you can analyze data from multiple sources in a single query.

In addition to ad hoc analysis, Log Analytics provides multiple ways to report and analyze data from a query.

- **Views and dashboards.** Views and dashboards visualize the results of a query in the portal. Management solutions will typically include views that analyze the data from the solution. You can also create your own custom views to analyze data and make it readily available in your custom portal.
- **Export.** You have the option to export the results of any query so that you can analyze it outside of Log Analytics. You can even schedule a regular export to Power BI which provides significant visualization and analysis capabilities.
- **Log Search API.** Log Analytics has a REST API for collecting data from any client. This allows you to programmatically work with data collected in the repository or access it from another monitoring tool.

Alerting

Log Analytics can proactively alert you or take corrective action when it detects an issue. Like all other analysis in Log Analytics, this is done with a log search. This search runs on a regular schedule, and an alert is created if the results match particular criteria.

In addition to creating an alert record in the Log Analytics repository, alerts can take the following actions.

- **Email.** Send an email to proactively notify you of a detected issue.
- **Runbook.** An alert in Log Analytics can start a runbook in Azure Automation. This is typically done to attempt to correct the detected issue. The runbook can be started in the cloud in the case of an issue in Azure or another cloud, or it could be started on a local agent for an issue on a physical or virtual machine.
- **Webhook.** An alert can start a webhook and pass it data from the results of the log search. This allows integration with external services such as an alternate alerting system, or it may attempt to take corrective action for an external web site.

Azure Automation

Azure Automation provides process automation and configuration management to OMS. It automates manual processes and helps to enforce configurations for physical and virtual computers.

Process Automation

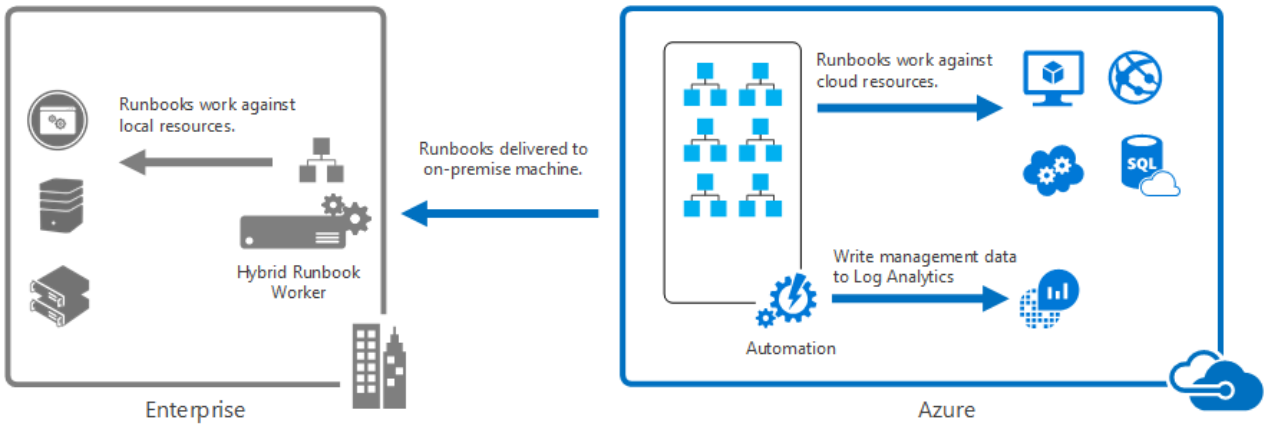
Azure Automation automates manual processes using runbooks which are based on PowerShell script or PowerShell workflow. It also includes assets supporting runbooks such as variables that can be shared between multiple runbooks and credentials and connections that allow you to store encrypted information that might be required for a runbook for authentication. Runbooks offer process automation for the other services in the suite. Since each of the other services can be accessed with PowerShell or through a REST API, you can create runbooks to perform such functions as collecting management data in Log Analytics or initiating a backup with Azure Backup.

Accessing resources

Since runbooks are based on PowerShell, they can manage any resource that can be accessed with PowerShell cmdlets. When you load a module into your Automation account, it becomes available to all runbooks in that account.

When runbooks run in the cloud, they can access any resources accessible from the cloud. This could be resources in your Azure subscription, in another cloud such as Amazon Web Services (AWS), or a service accessible through a REST API. Runbooks in the cloud don't run under any credentials, but they can leverage Automation assets such as credentials, connections, and certificates to authenticate to resources they access.

Resources in your data center most likely cannot be accessed from a runbook running in the cloud. You can install one or more Hybrid Runbook Workers in your data center though to run runbooks that require access to local resources. When you start a runbook, you specify whether it should run in the cloud or on a specific worker.



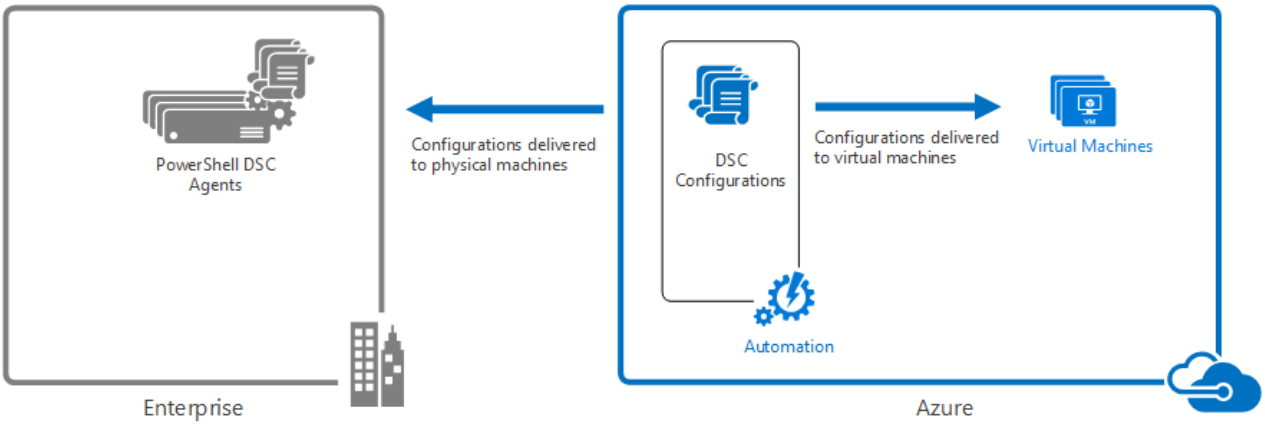
Starting a runbook

Runbooks can be started through a number of methods so that they can be included in a variety of management scenarios.

- **Azure Portal.** Like other Azure services, Azure Automation can be managed from the Azure Portal. In addition to starting runbooks, you can import them or author your own.
- **Scheduled.** You can schedule runbooks to start at regular intervals. This allows you to automatically repeat a regular management process or collect data to Log Analytics.
- **PowerShell and API.** You can start runbooks and pass them required parameter information from a PowerShell cmdlet or the Azure Automation REST API.
- **Webhook.** A webhook can be created for any runbook that allows it to be started from external applications or web sites.
- **Log Analytics Alert.** An alert in Log Analytics can automatically start a runbook to attempt to correct the issue identified by the alert.

Configuration Management

PowerShell Desired State Configuration (DSC) is a management platform in Windows PowerShell that allows you to deploy and enforce the configuration of physical and virtual machines. Azure Automation manages DSC configurations and provides a pull server in the cloud that agents can access to retrieve required configurations.



Azure Backup and Azure Site Recovery

Azure Backup and Azure Site Recovery contribute to business continuity and disaster recovery. They each have features that help you to ensure that applications remain available when outages occur and return to normal operations when systems come back online. Both services contribute to the recovery point objectives (RPOs) and recovery time objectives (RTOs) defined for your organization. Your RPO defines the acceptable limit in which data isn't available during an outage, and the RTO limits the acceptable amount of time in which a service or app isn't available during an outage.

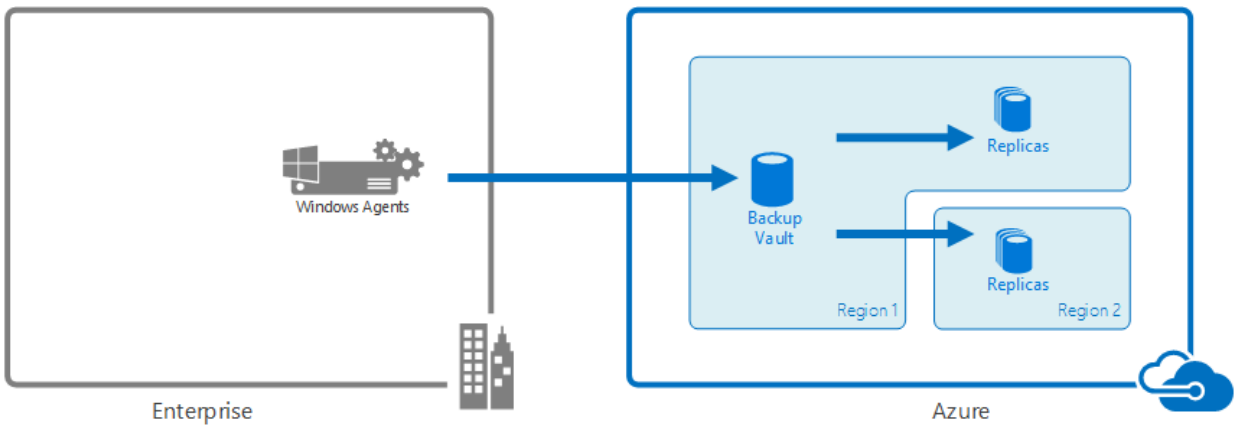
Azure Backup

Azure Backup provides data backup and restore services for OMS. It protects your application data and retains it for years without any capital investment and with minimal operating costs. It can backup data from physical and virtual Windows servers in addition to application workloads such as SQL Server and SharePoint. It can also be used by System Center Data Protection Manager (DPM) to replicate protected data to Azure for redundancy and long term storage.

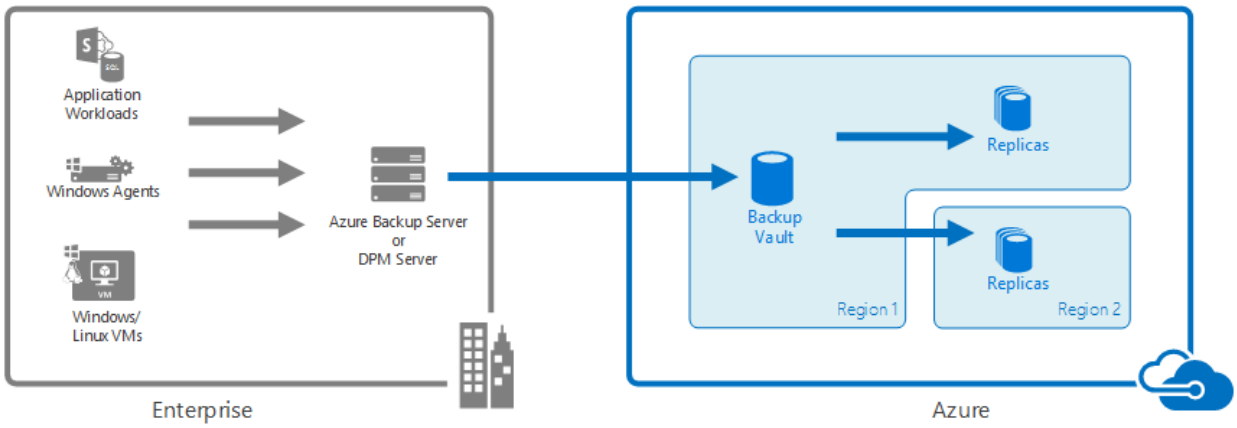
Protected data in Azure Backup is stored in a backup vault located in a particular geographic region. The data is replicated within the same region and, depending on the type of vault, may also be replicated to another region for further resiliency .

Azure Backup has three fundamental scenarios.

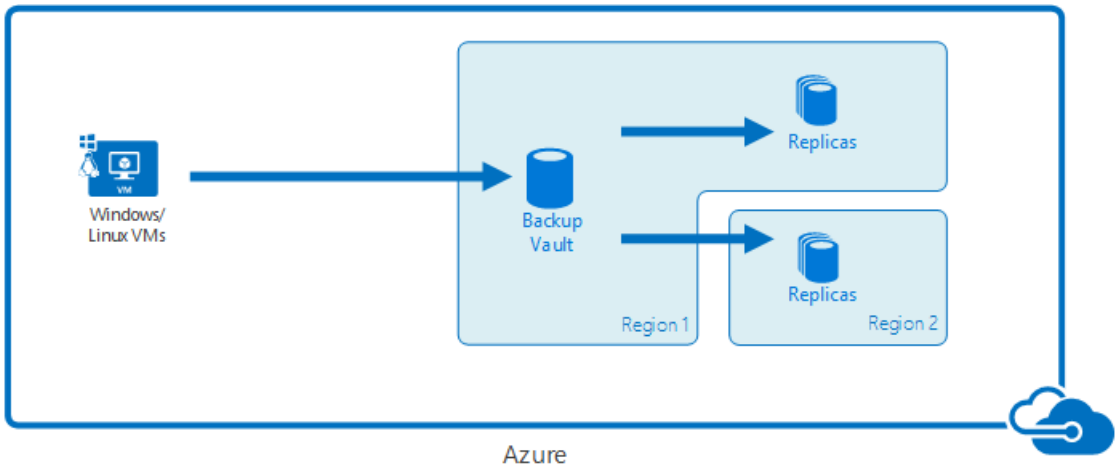
- **Windows machine with Azure Backup agent.** Backup files and folders from any Windows server or client directly to your Azure backup vault.



- **System Center Data Protection Manager (DPM) or Microsoft Azure Backup Server.** Leverage DPM or Microsoft Azure Backup Server to backup files and folders in addition to application workloads such as SQL and SharePoint to local storage and then replicate to your Azure backup vault. Supports Windows and Linux virtual machines on Hyper-V or VMware.



- **Azure Virtual Machine Extensions.** Backup Windows or Linux virtual machines in Azure to your Azure backup vault.



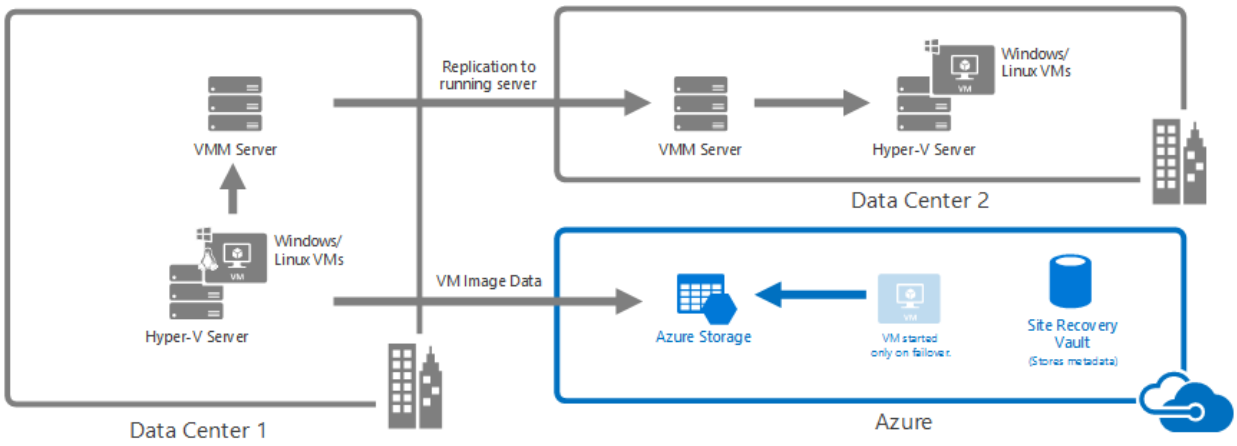
Azure Site Recovery

Azure Site Recovery provides business continuity by orchestrating replication of on-premises virtual and physical machines to Azure, or to a secondary site. If your primary site is unavailable, you fail over to the secondary location so that users can keep working, and fail back when systems return to working order.

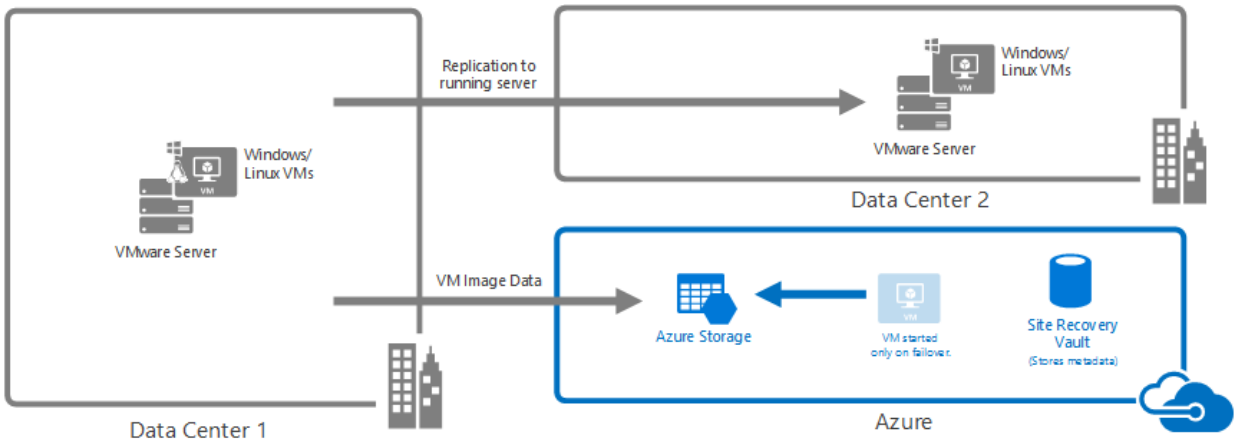
Azure Site Recovery provides high availability for servers and applications. It contributes to your business continuity and a disaster recovery (BCDR) strategy by orchestrating replication, failover, and recovery of on-premises Hyper-V virtual machines, VMware virtual machines, and physical Windows/Linux servers. You can replicate machines to a secondary data center or extend your data center by replicating them to Azure. Site Recovery also provides simple failover and recovery for workloads. It integrates with disaster recovery mechanisms such as SQL Server AlwaysOn, and provides recovery plans for easy failover of workloads that are tiered across multiple machines.

Azure Site Recovery has three fundamental replication scenarios.

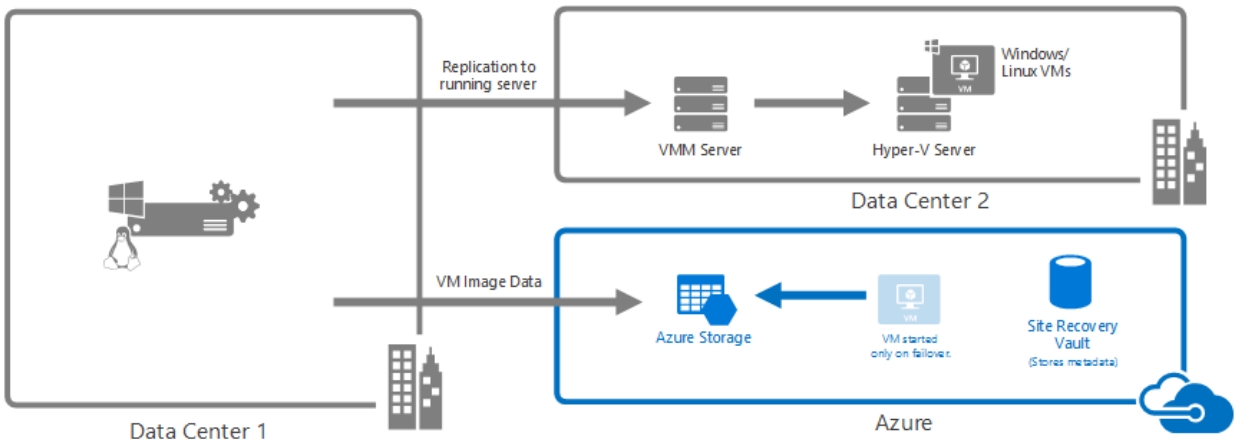
- **Replication of Hyper-V virtual machines.** If Hyper-V virtual machines are managed in VMM clouds, you can replicate to a secondary data center or to Azure storage. Replication to Azure is over a secure internet connection. Replication to a secondary datacenter is over the LAN. If Hyper-V virtual machines aren't managed by VMM, you can replicate to Azure storage only. Replication to Azure is over a secure internet connection.



- **Replication of VMware virtual machines.** You can replicate VMware virtual machines to a secondary datacenter running VMware or to Azure storage. Replication to Azure can occur over a site-to-site VPN or Azure ExpressRoute or over a secure Internet connection. Replication to a secondary datacenter occurs over the InMage Scout data channel.



- **Replication of physical Windows and Linux servers.** You can replicate physical servers to a secondary datacenter or to Azure storage. Replication to Azure can occur over a site-to-site VPN or Azure ExpressRoute or over a secure Internet connection. Replication to a secondary datacenter occurs over the InMage Scout data channel. Azure Site Recovery has an OMS solution that displays some statistics, but you must use the Azure portal for any operations.



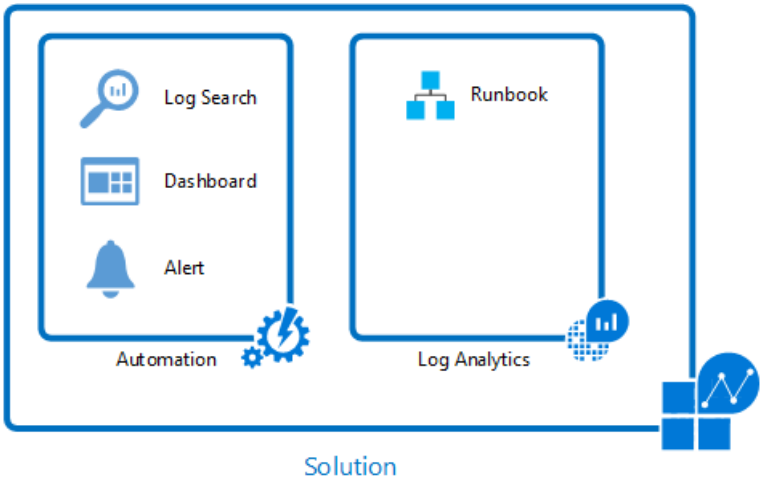
Site Recovery stores metadata in vaults located in a particular geographic Azure region. No replicated data is stored by the Site Recovery service .

Management Solutions

Management Solutions are prepackaged sets of logic that implement a particular management scenario

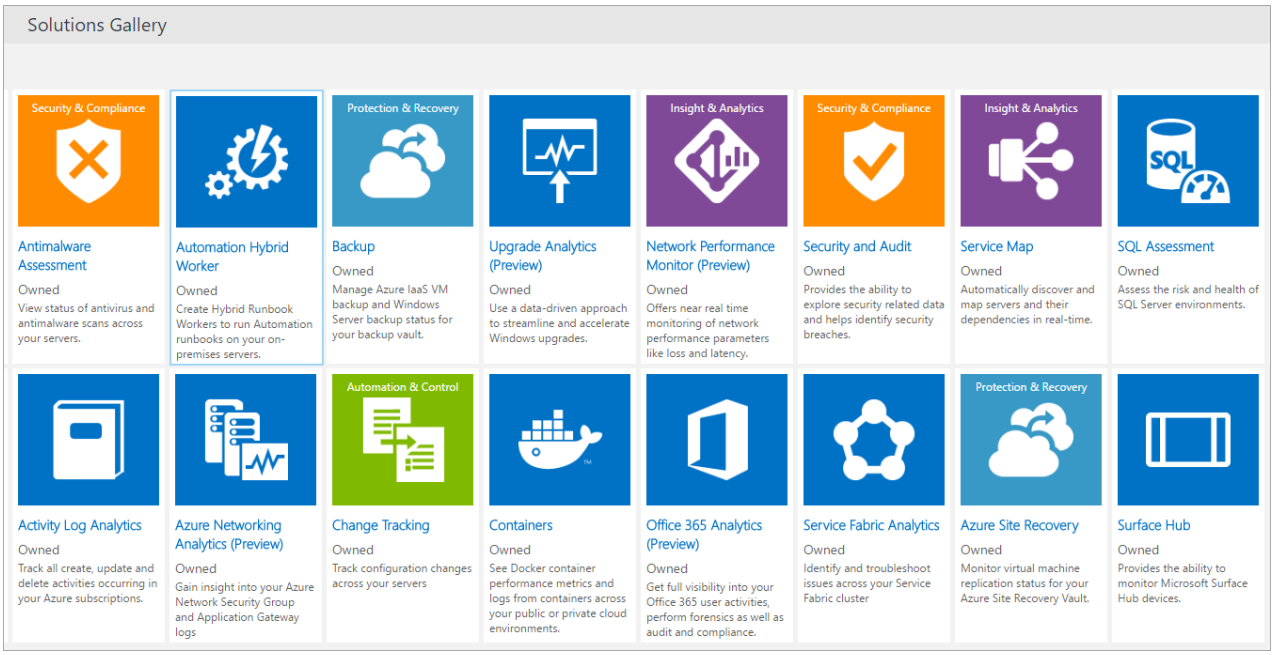
leveraging one or more OMS services. Different solutions are available from Microsoft and from partners that you can easily add to your Azure subscription to increase the value of your investment in OMS. As a partner you can create your own solutions to support your applications and services and provide them to users through the Azure Marketplace or Quickstart Templates.

A good example of a solution that leverages multiple services to provide additional functionality is the Update Management solution. 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 with 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 don't need to worry about the underlying details.



Most solutions may perform one or more of the following functions.

- Collect additional information. Log Analytics collects a variety of data from clients and services including events and performance data. A management solution may collect additional information not available from other data sources, often using Azure Automation runbooks.
- Provide additional analysis of collected information. Management solutions include dashboards and views that provide analysis and visualization of data. These link back to predefined log searches that allow you to drill into the detailed data. They may also perform analysis on data that's already been collected into the repository, for example searching across security events for patterns that indicate a threat.
- Add functionality. Some solutions provided by Microsoft may build upon the capabilities of the core services to provide additional functionality. Service Map for example provides its own console to discover and maps server and process dependencies in real time. Solutions are regularly being added to OMS by Microsoft and partners allowing you to continuously increase the value of your investment. You can browse and install Microsoft solutions through the Solutions Catalog in the OMS portal or browse and install both Microsoft and partner solutions through the Azure Marketplace in the Azure Portal.



Next steps

- Learn about Log Analytics.
- Learn about Azure Automation.
- Learn about Azure Backup.
- Learn about Azure Site Recovery.
- Discover the solutions that are available in the different OMS offerings.

OMS architecture

4/12/2017 • 3 min to read • Edit Online

Operations Management Suite (OMS) is a collection of cloud-based services for managing your on-premises and cloud environments. This article describes the different on-premises and cloud components of OMS and their high level cloud computing architecture. You can refer to the documentation for each service for further details.

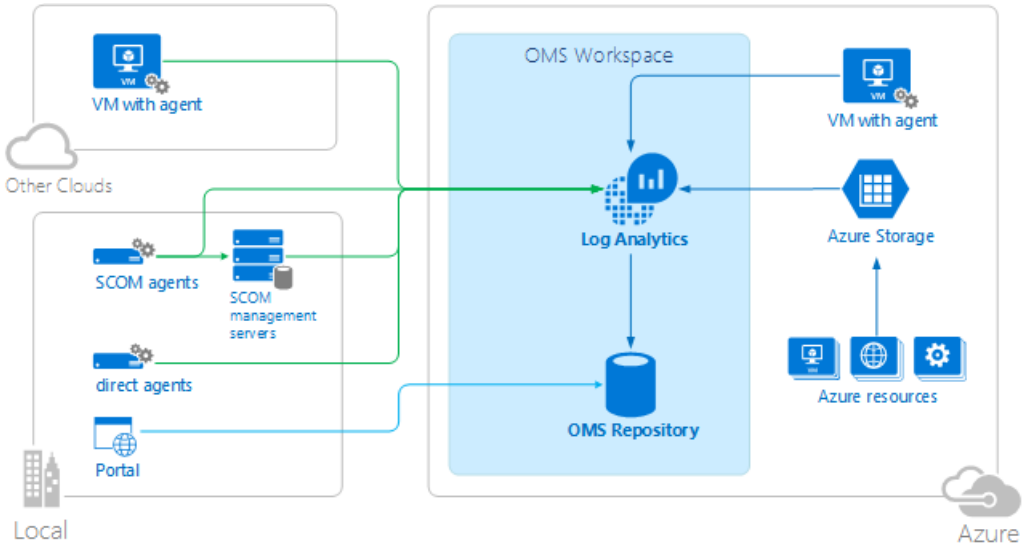
Log Analytics

All data collected by Log Analytics is stored in the OMS repository which is hosted in Azure. Connected Sources generate data collected into the OMS repository. There are currently three types of connected sources supported.

- An agent installed on a Windows or Linux computer connected directly to OMS.
- A System Center Operations Manager (SCOM) management group connected to Log Analytics . SCOM agents continue to communicate with management servers which forward events and performance data to Log Analytics.
- An Azure storage account that collects Azure Diagnostics data from a worker role, web role, or virtual machine in Azure.

Data sources define the data that Log Analytics collects from connected sources including event logs and performance counters. Solutions add functionality to OMS and can easily be added to your workspace from the OMS Solutions Gallery. Some solutions may require a direct connection to Log Analytics from SCOM agents while others may require an additional agent to be installed.

Log Analytics has a web-based portal that you can use to manage OMS resources, add and configure OMS solutions, and view and analyze data in the OMS repository.

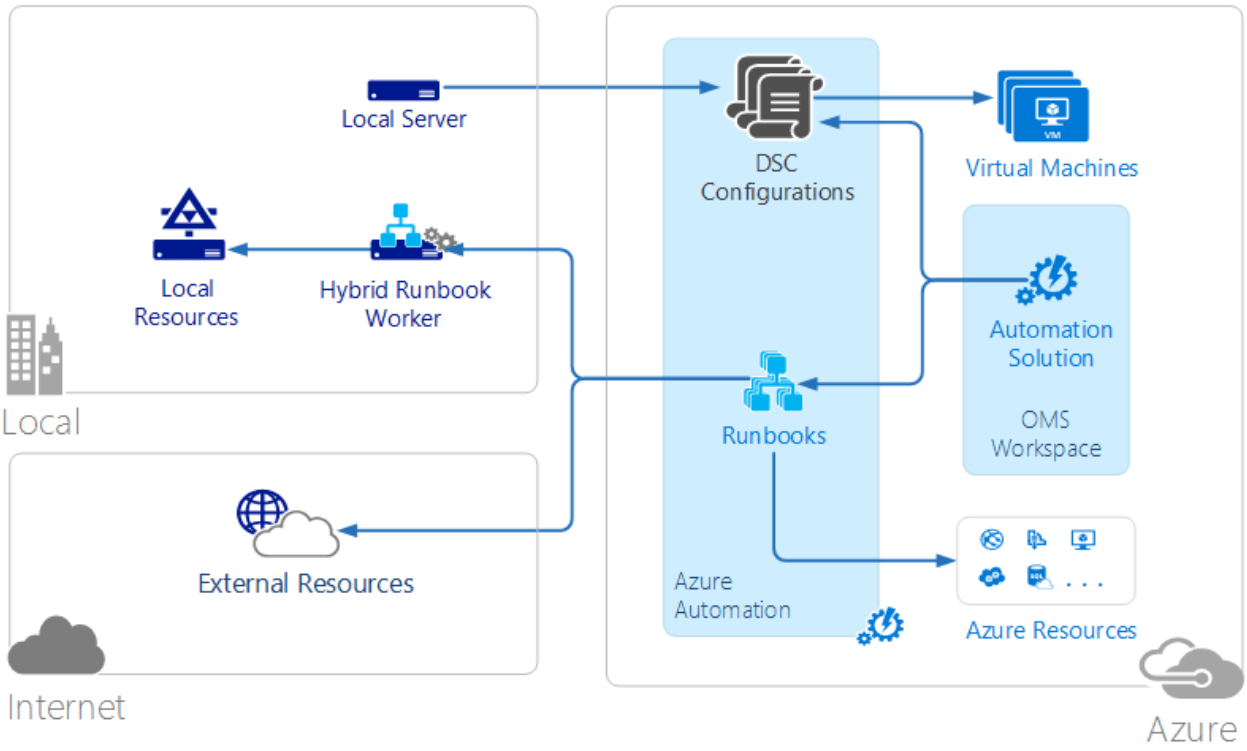


Azure Automation

Azure Automation runbooks are executed in the Azure cloud and can access resources that are in Azure, in other cloud services, or accessible from the public Internet. You can also designate on-premises machines in your local data center using Hybrid Runbook Worker so that runbooks can access local resources.

DSC configurations stored in Azure Automation can be directly applied to Azure virtual machines. Other physical and virtual machines can request configurations from the Azure Automation DSC pull server.

Azure Automation has an OMS solution that displays statistics and links to launch the Azure portal for any operations.



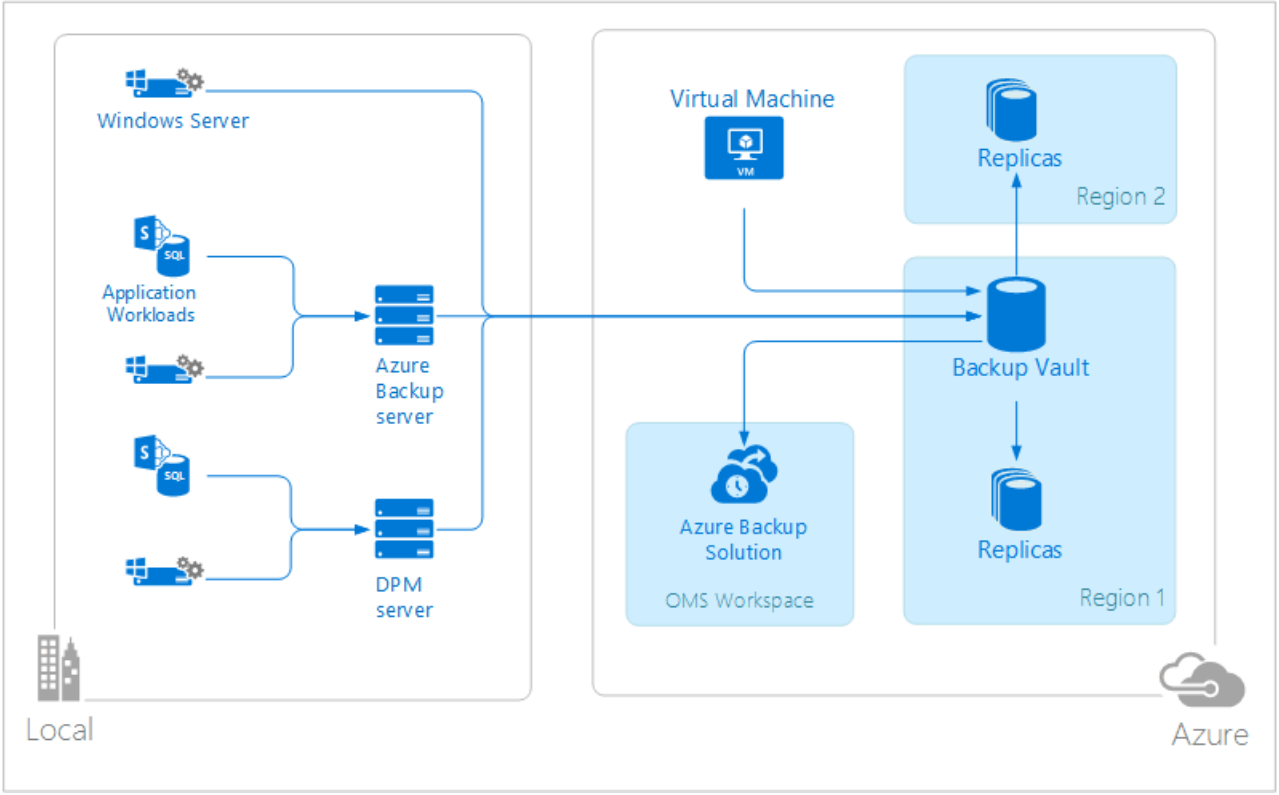
Azure Backup

Protected data in Azure Backup is stored in a backup vault located in a particular geographic region. The data is replicated within the same region and, depending on the type of vault, may also be replicated to another region for further redundancy.

Azure Backup has three fundamental scenarios.

- Windows machine with Azure Backup agent. This allows you to backup files and folders from any Windows server or client directly to your Azure backup vault.
- System Center Data Protection Manager (DPM) or Microsoft Azure Backup Server. This allows you to leverage DPM or Microsoft Azure Backup Server to backup files and folders in addition to application workloads such as SQL and SharePoint to local storage and then replicate to your Azure backup vault.
- Azure Virtual Machine Extensions. This allows you to backup Azure virtual machines to your Azure backup vault.

Azure Backup has an OMS solution that displays statistics and links to launch the Azure portal for any operations.



Azure Site Recovery

Azure Site Recovery orchestrates replication, failover, and failback of virtual machines and physical servers. Replication data is exchanged between Hyper-V hosts, VMware hypervisors, and physical servers in primary and secondary datacenters, or between the datacenter and Azure storage. Site Recovery stores metadata in vaults located in a particular geographic Azure region. No replicated data is stored by the Site Recovery service.

Azure Site Recovery has three fundamental replication scenarios.

Replication of Hyper-V virtual machines

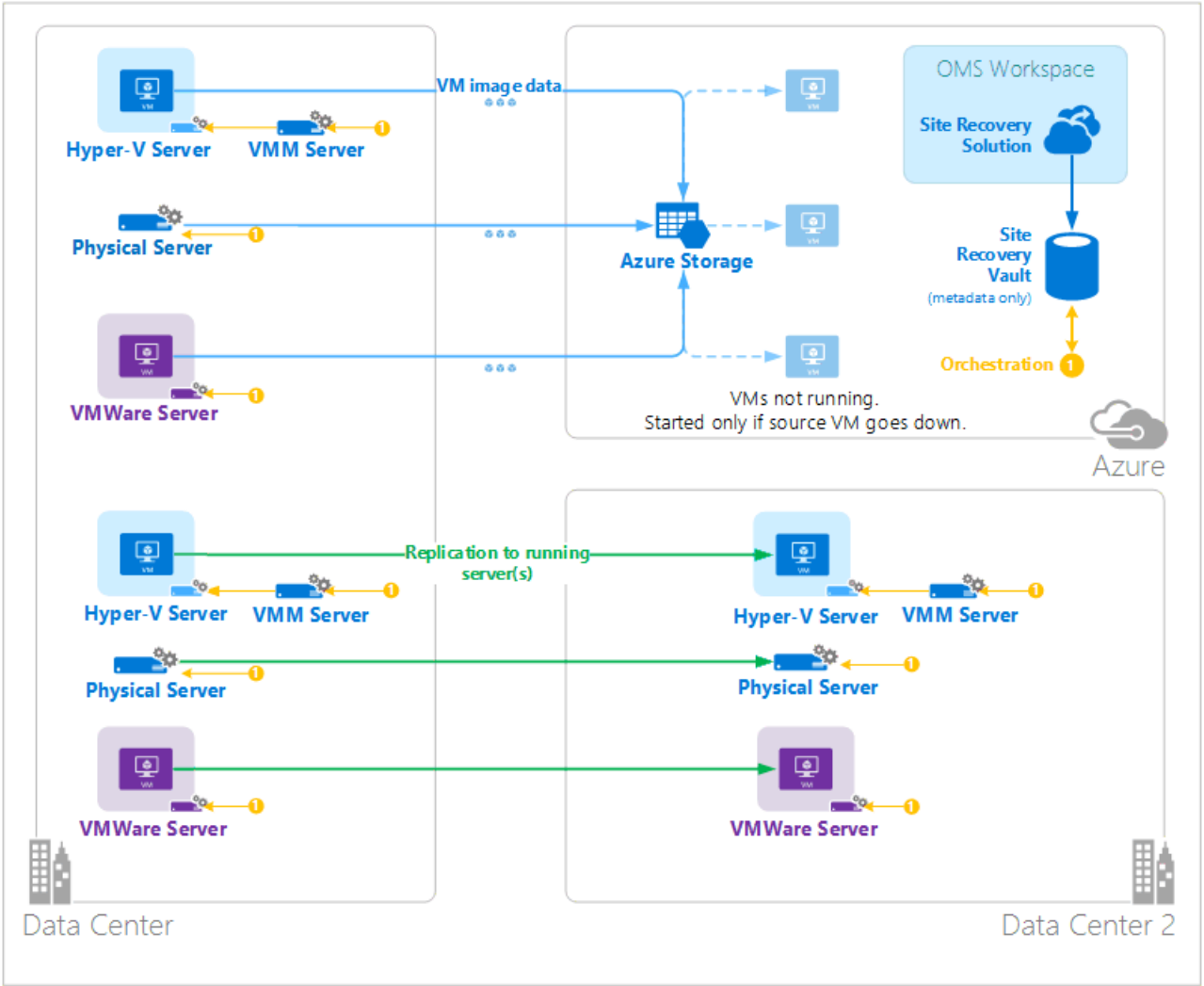
- If Hyper-V virtual machines are managed in VMM clouds, you can replicate to a secondary data center or to Azure storage. Replication to Azure is over a secure internet connection. Replication to a secondary datacenter is over the LAN.
- If Hyper-V virtual machines aren't managed by VMM, you can replicate to Azure storage only. Replication to Azure is over a secure internet connection.

Replication of VMWare virtual machines

- You can replicate VMware virtual machines to a secondary datacenter running VMware or to Azure storage. Replication to Azure can occur over a site-to-site VPN or Azure ExpressRoute or over a secure Internet connection. Replication to a secondary datacenter occurs over the InMage Scout data channel.

Replication of physical Windows and Linux servers

- You can replicate physical servers to a secondary datacenter or to Azure storage. Replication to Azure can occur over a site-to-site VPN or Azure ExpressRoute or over a secure Internet connection. Replication to a secondary datacenter occurs over the InMage Scout data channel. Azure Site Recovery has an OMS solution that displays some statistics, but you must use the Azure portal for any operations.



Next steps

- Learn about Log Analytics.
- Learn about Azure Automation.
- Learn about Azure Backup.
- Learn about Azure Site Recovery.

Operations Management Suite (OMS) self paced demo - Service Map

4/12/2017 • 5 min to read • Edit Online

This is a self paced demo that walks through using the Service Map solution in Operations Management Suite (OMS) to identify and diagnose a simulated problem in a web application. Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. It also consolidates data collected by other OMS services to assist you in analyzing performance and identifying issues. You'll also use log searches in Log Analytics to drill down on collected data in order to identify the root problem.

Scenario description

You've just received a notification that the ACME Customer Portal application is having performance issues. The only information that you have is that these issues started about 4:00 am PST today. You aren't entirely sure of all the components that the portal is dependent on other than a set of web servers.

Components and features used

- Service Map solution
- Log Analytics log searches

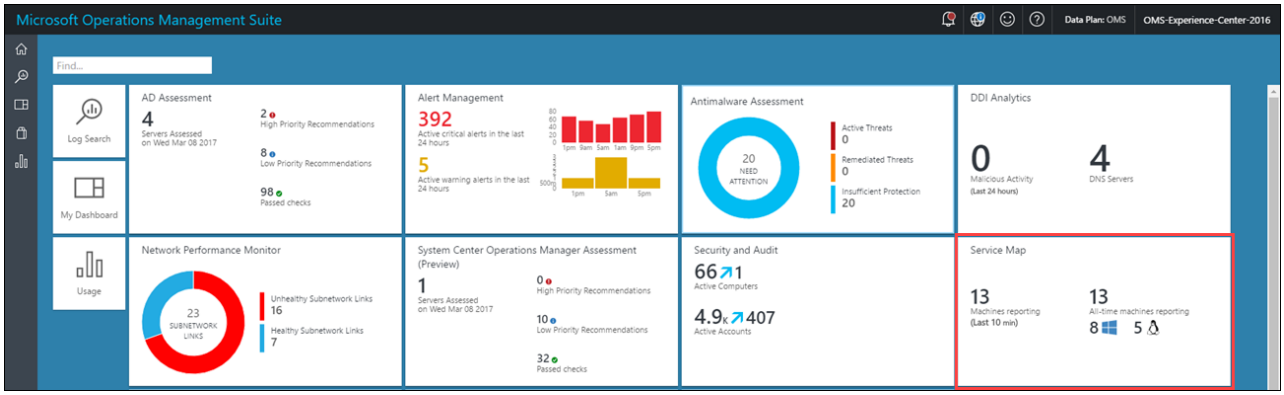
Walk through

1. Connect to the OMS Experience Center

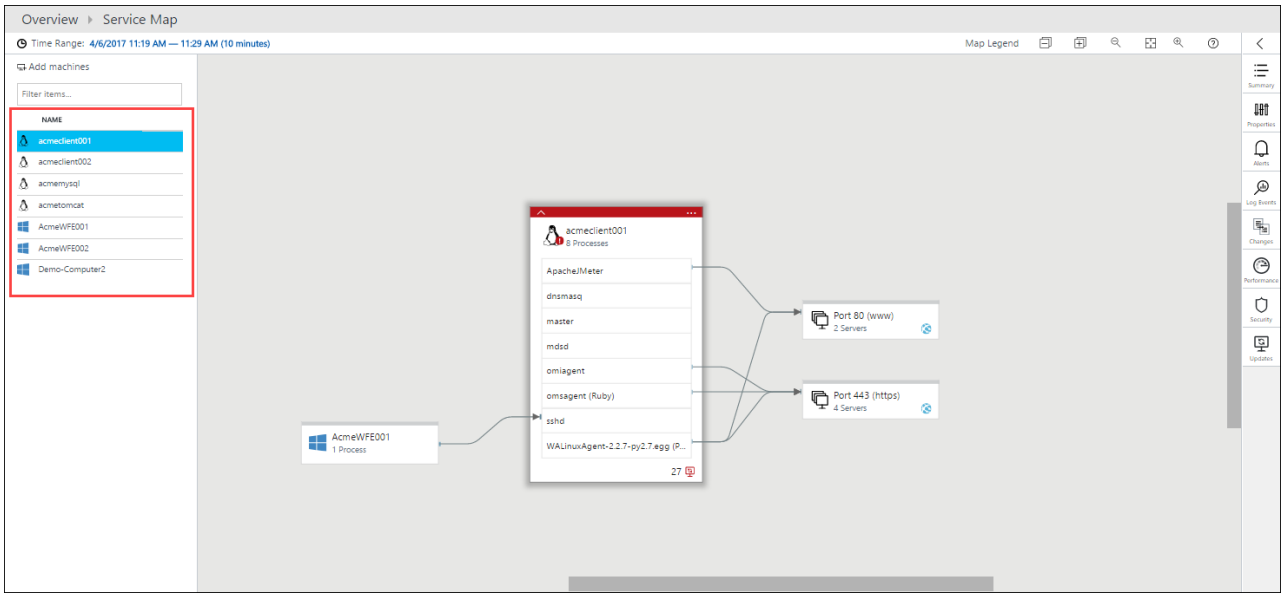
This walk through uses the Operations Management Suite Experience Center which provides a complete OMS environment with sample data. Start by following this link, provide your information and then select the **Insight and Analytics** scenario.

2. Start Service Map

Start the Service Map solution by clicking on the **Service Map** tile.

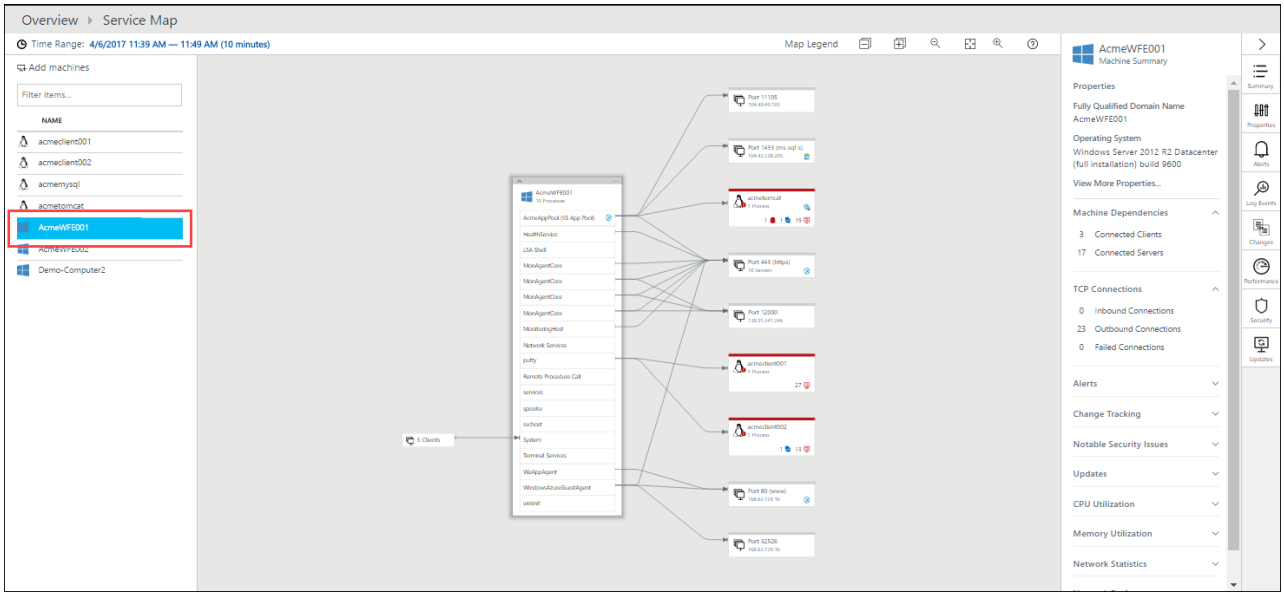


The Service Map console is displayed. In the left pane is a list of computers in your environment with the Service Map agent installed. You'll select the computer that you want to view from this list.

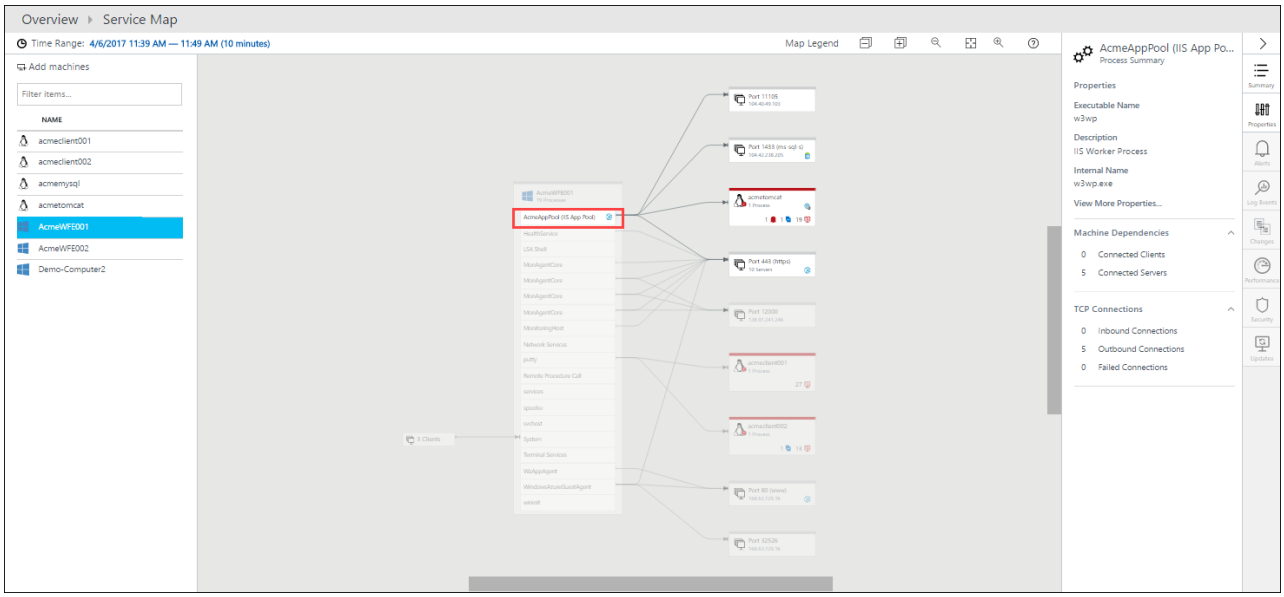


3. View computer

We know that the web servers are called AcmeWFE001 and AcmeWFE002, so this seems like a reasonable place to start. Click on **AcmeWFE001**. This displays the map for AcmeWFE001 and all of its dependencies. You can see which processes are running on the selected computer and which external services they communicate with.

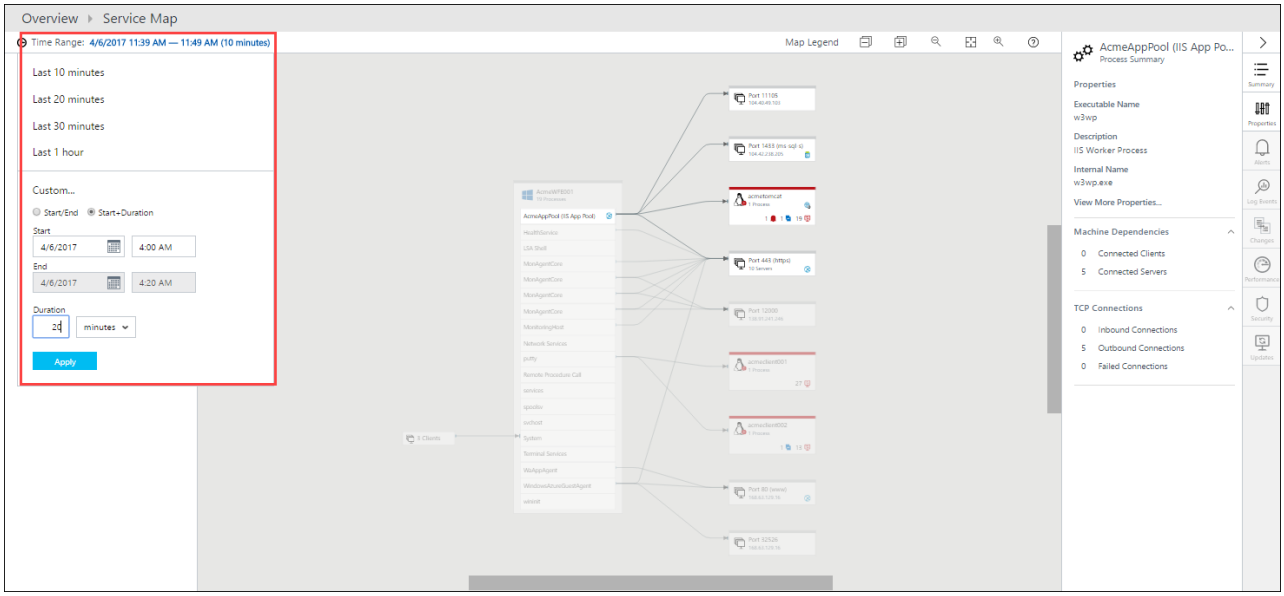


We're concerned about the performance of our web application so click on the **AcmeAppPool (IIS App Pool)** process. This displays the details for this process and highlights its dependencies.



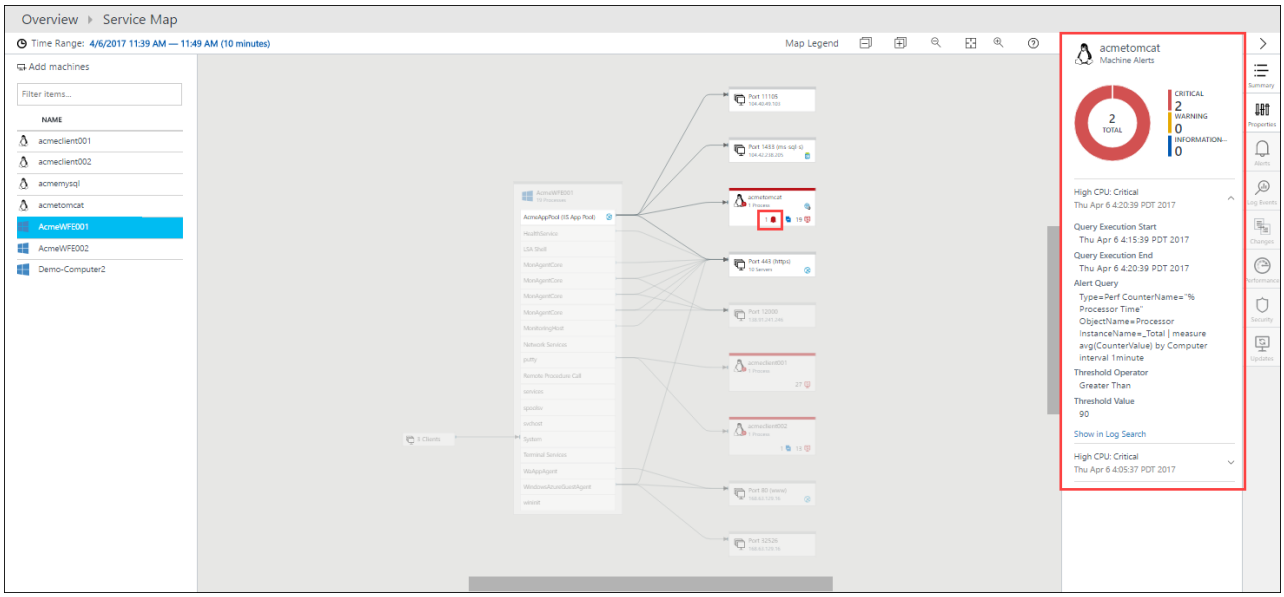
4. Change time window

We heard that the problem started at 4:00 AM so let's have a look at what was happening at that time. Click on **Time Range** and change the time to 4:00 AM PST (keep the current date and adjust for your local time zone) with a duration of 20 minutes.



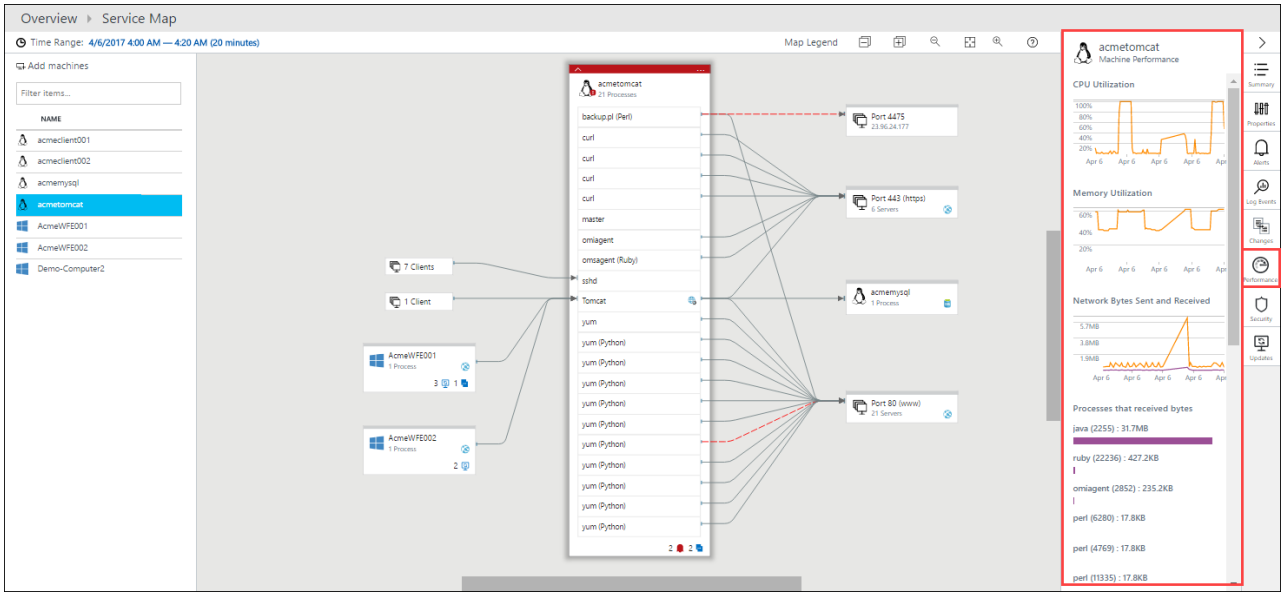
5. View alert

We now see that the **acmetomcat** dependency has an alert displayed, so that's our potential problem. Click on the alert icon in **acmetomcat** to show the details for the alert. We can see that we have critical CPU utilization and can expand it for more detail. This is probably what's causing our slow performance.



6. View performance

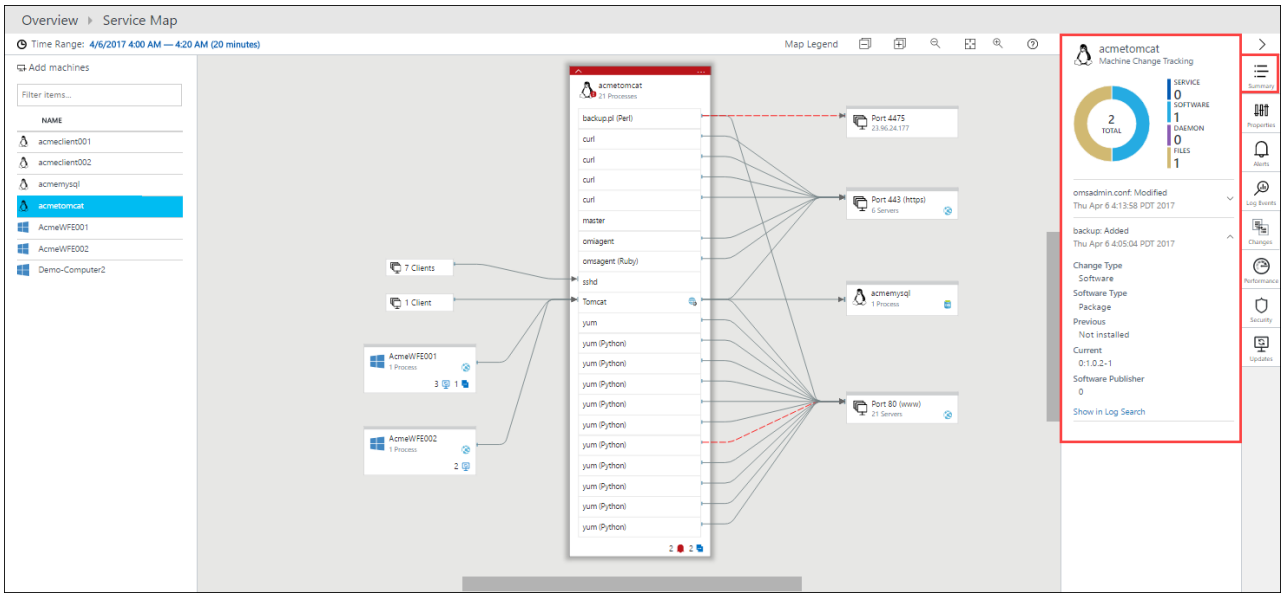
Let's have a closer look at **acmetomcat**. Click in the top right of **acmetomcat** and select **Load Server Map** to show the detail and dependencies for this machine. We can then look a bit more into those performance counters to verify our suspicion. Select the **Performance** tab to display the performance counters collected by Log Analytics over the time range. We can see that we're getting periodic spikes in the processor and memory.



7. View change tracking

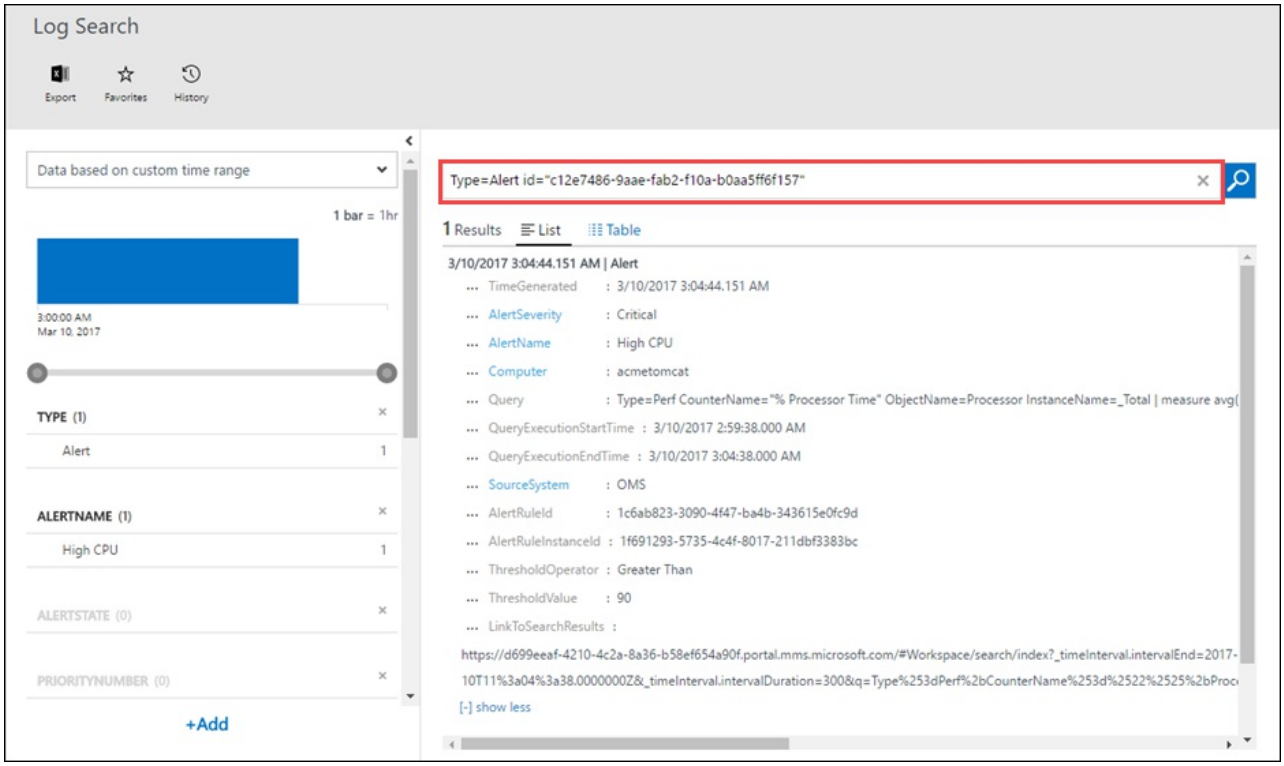
Let's see if we can find out what might have caused this high utilization. Click on the **Summary** tab. This provides information that OMS has collected from the computer such as failed connections, critical alerts, and software changes. Sections with interesting recent information should already be expanded, and you can expand other sections to inspect information that they contain.

If **Change Tracking** isn't already open, then expand it. This shows information collected by the Change Tracking solution. It looks like there was a software change made during this time window. Click on **Software** to get details. A backup process was added to the machine just after 4:00 AM, so this appears to be the culprit for the excessive resources being consumed.



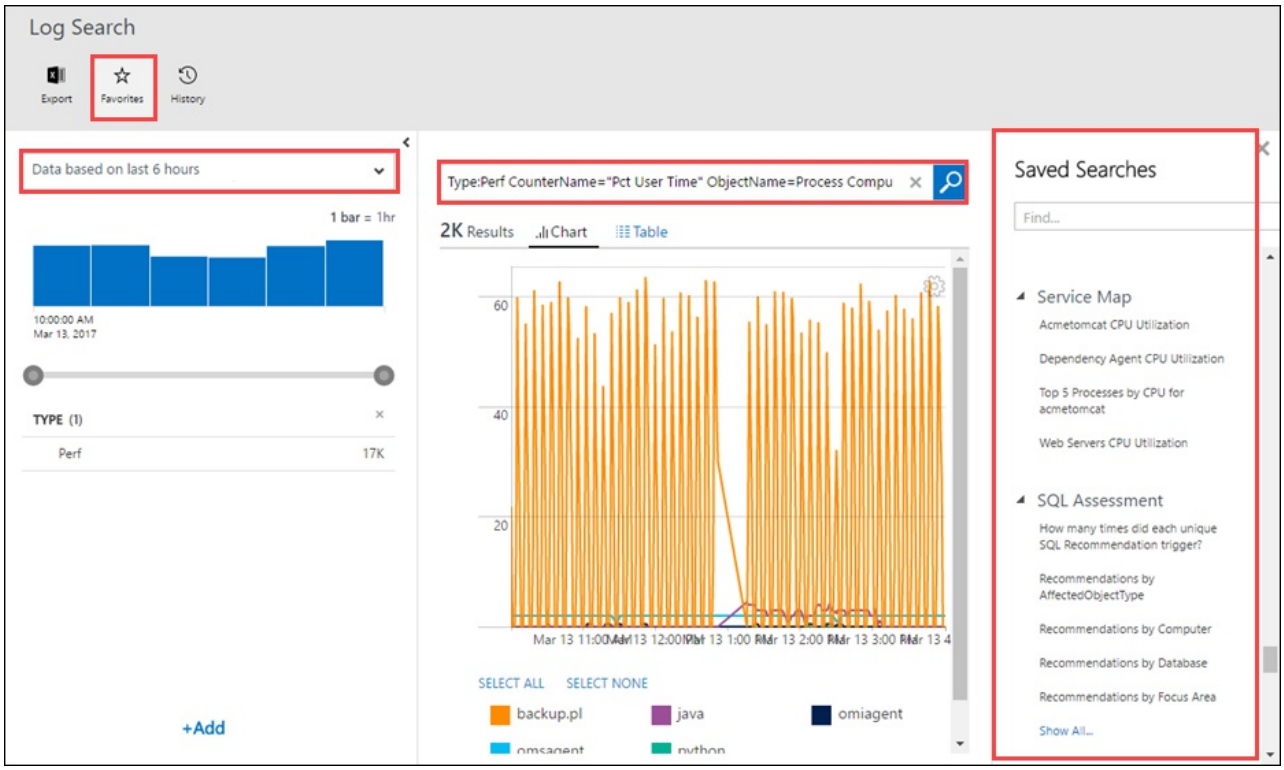
8. View details in Log Search

We can further verify this by looking at the detailed performance information collected in the Log Analytics repository. Click on the **Alerts** tab again and then on one of the **High CPU** alerts. Click on **Show in Log Search**. This opens the Log Search window where you can perform log searches against any data stored in the repository. Service Map already filled in a queriy for us to retrieve the alert we're interested in.



9. Open saved search

Let's see if we can get some more detail on the performance collection that generated this alert and verify our suspicion that the problems are being caused by that backup process. Change the time range to **6 hours**. Then click on **Favorites** and scroll down to the saved searches for **Service Map**. These are queries that we created specifically for this analysis. Click on **Top 5 Processes by CPU for acmetomcat**.



This query returns a list of the top 5 processes consuming processor on **acmetomcat**. You can inspect the query to get an introduction to the query language used for log searches. If you were interested in the processes on other computers, you could modify the query to retrieve that information.

In this case, we can see that the backup process is consistently consuming about 60% of the app server's CPU. It's pretty obvious that this new process is responsible for our performance problem. Our solution would obviously be to remove this new backup software off the application server. We could actually leverage Desired State Configuration (DSC) managed by Azure Automation to define policies that ensure this process never runs on these critical systems.

Summary points

- Service Map provides you with a view of your entire application even if you don't know all of its servers and dependencies.
- Service Map surfaces data collected by other OMS solutions to help you identify issues with your application and its underlying infrastructure.
- Log searches allow you to drill down into specific data collected in the Log Analytics repository.

Next steps

- Learn more about Service Map.
- Deploy and configure Service Map.
- Learn about Log Analytics which is required for Service Map and stores operational data stored by agents.

What is Log Analytics?

4/20/2017 • 4 min to read • Edit Online

Log Analytics is a service in Operations Management Suite (OMS) that monitors your cloud and on-premises environments to maintain their availability and performance. It collects data generated by resources in your cloud and on-premises environments and from other monitoring tools to provide analysis across multiple sources. This article provides a brief discussion of the value that Log Analytics provides, an overview of how it operates, and links to more detailed content so you can dig further.

Is Log Analytics for you?

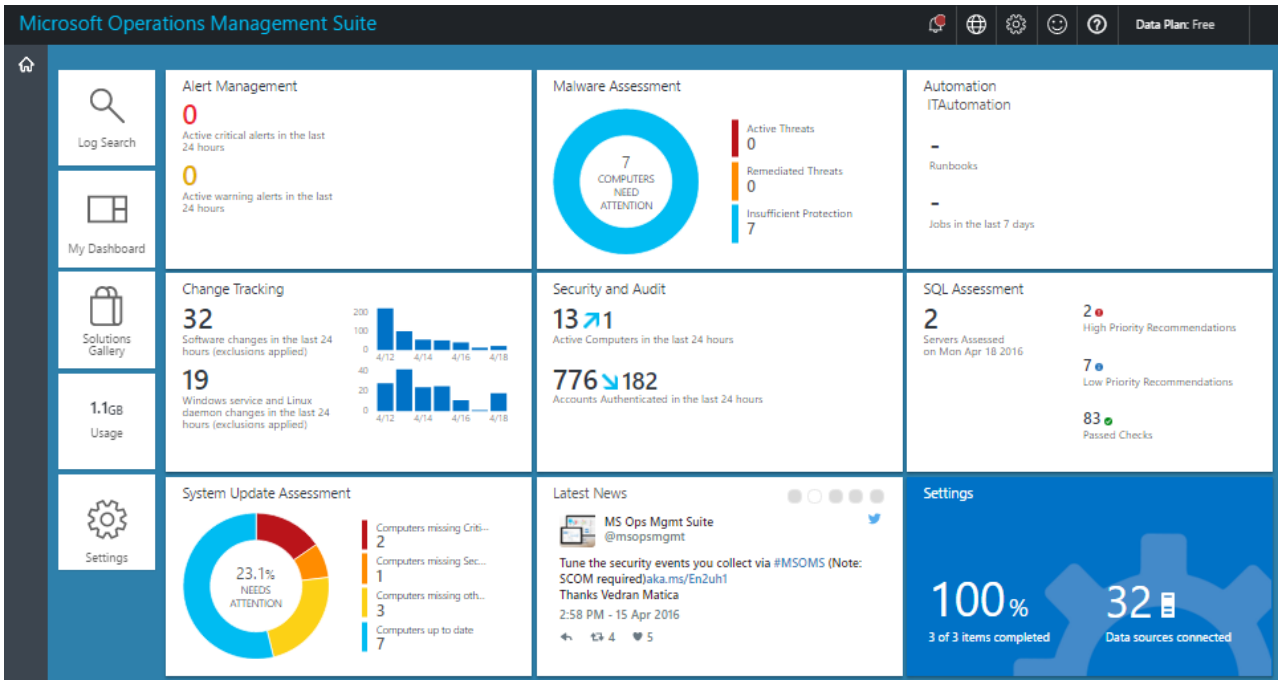
If you have no current monitoring in place for your Azure environment, you should start with Azure Monitor which collects and analyzes monitoring data for your Azure resources. Log Analytics can collect data from Azure Monitor to correlate it with other data and provide additional analysis.

If you want to monitor your on-premise environment or you have existing monitoring using services such as Azure Monitor or System Center Operations Manager, then Log Analytics can add significant value. It can collect data directly from your agents and also from these other tools into a single repository. Analysis tools in Log Analytics such as log searches, views, and solutions work against all collected data providing you with centralized analysis of your entire environment.

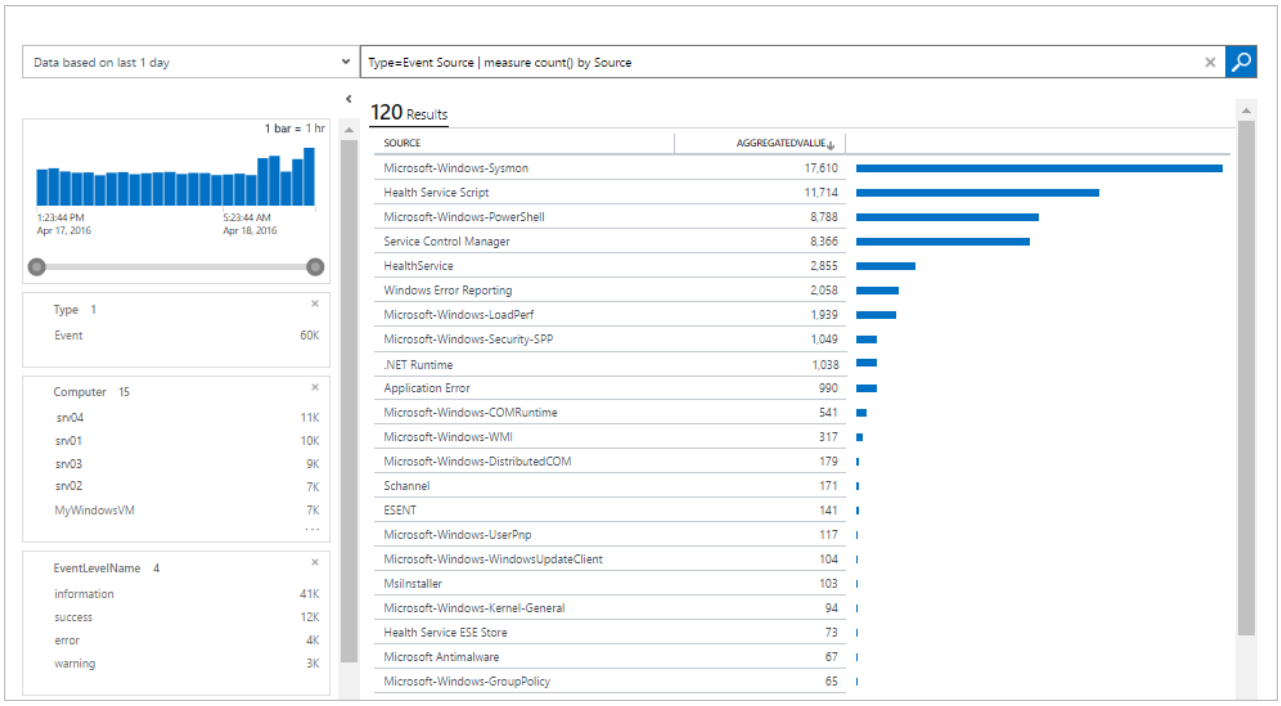
Using Log Analytics

You can access Log Analytics through the OMS portal or the Azure portal which run in any browser and provide you with access to configuration settings and multiple tools to analyze and act on collected data. From the portal you can leverage log searches where you construct queries to analyze collected data, dashboards which you can customize with graphical views of your most valuable searches, and solutions which provide additional functionality and analysis tools.

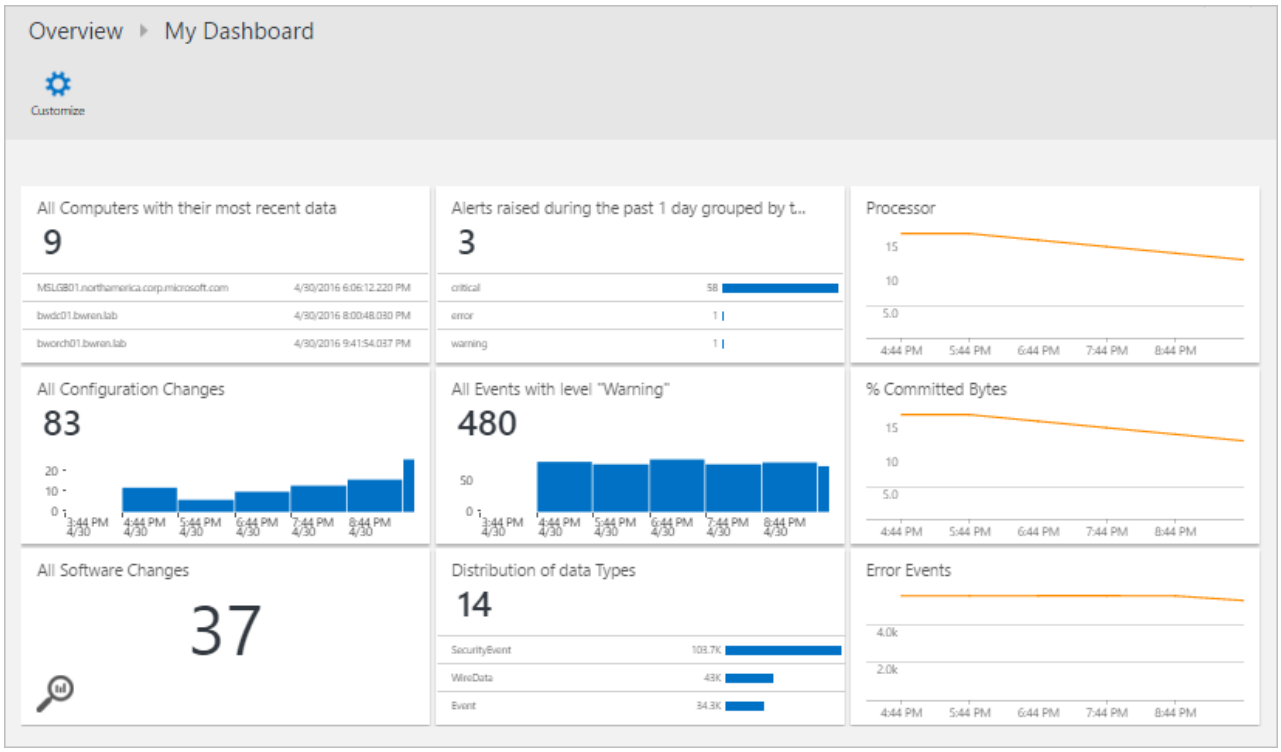
The image below is from the OMS portal which shows the dashboard that displays summary information for the solutions that are installed in the workspace. You can click on any tile to drill further into the data for that solution.



Log Analytics includes a query language to quickly retrieve and consolidate data in the repository. You can create and save Log Searches to directly analyze data in the portal or have log searches run automatically to create an alert if the results of the query indicate an important condition.



To get a quick graphical view of the health of your overall environment, you can add visualizations for saved log searches to your dashboard.

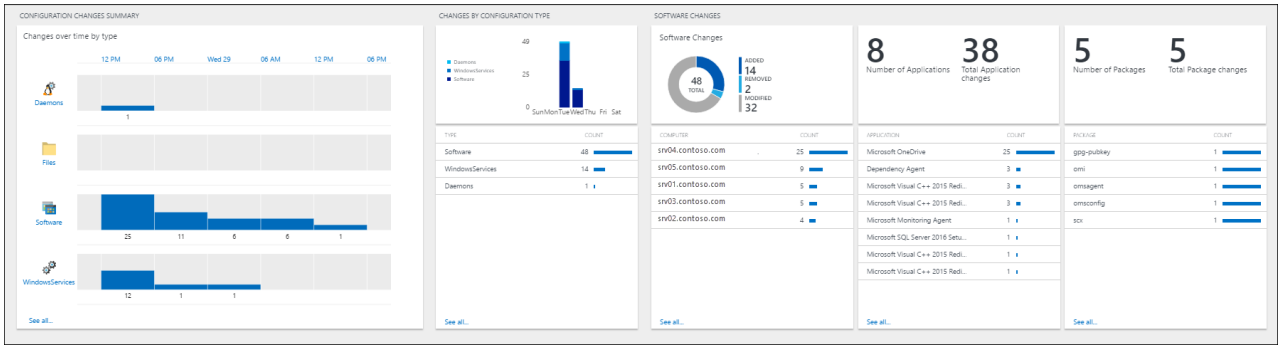


In order to analyze data outside of Log Analytics, you can export the data from the OMS repository into tools such as Power BI or Excel. You can also leverage the Log Search API to build custom solutions that leverage Log Analytics data or to integrate with other systems.

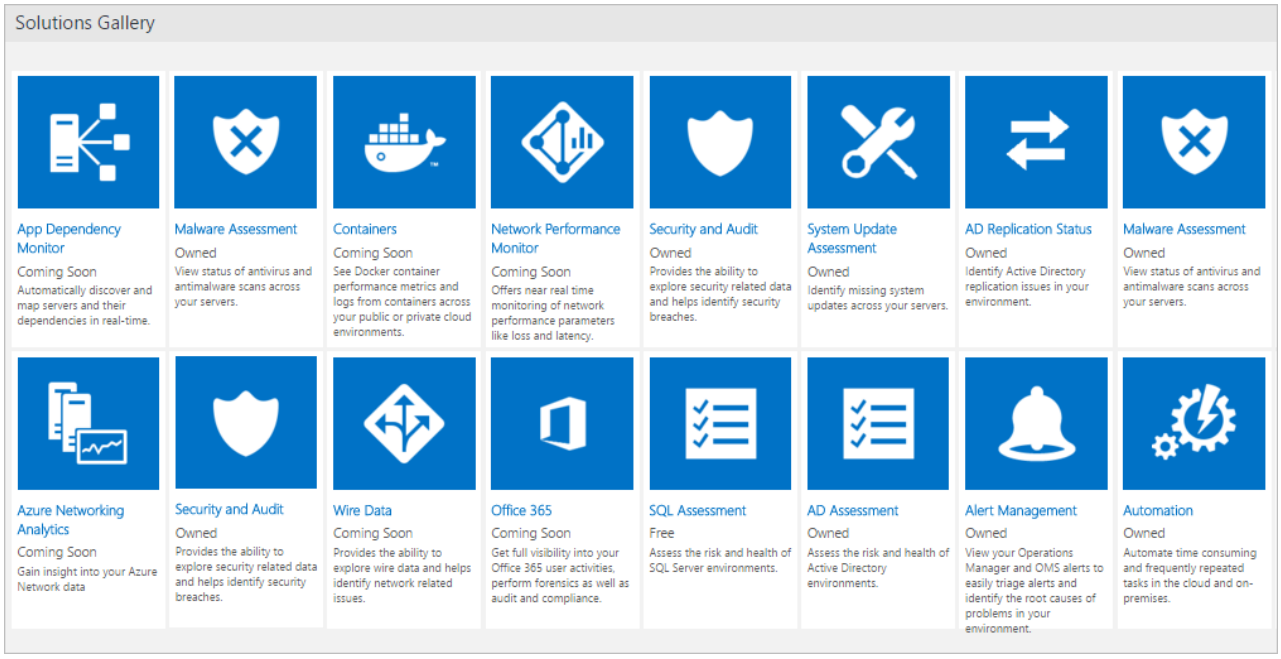
Add functionality with management solutions

Management solutions add functionality to OMS, providing additional data and analysis tools to Log Analytics. They may also define new record types to be collected that can be analyzed with Log Searches or by additional user

interface provided by the solution in the dashboard. The example image below shows the Change Tracking solution

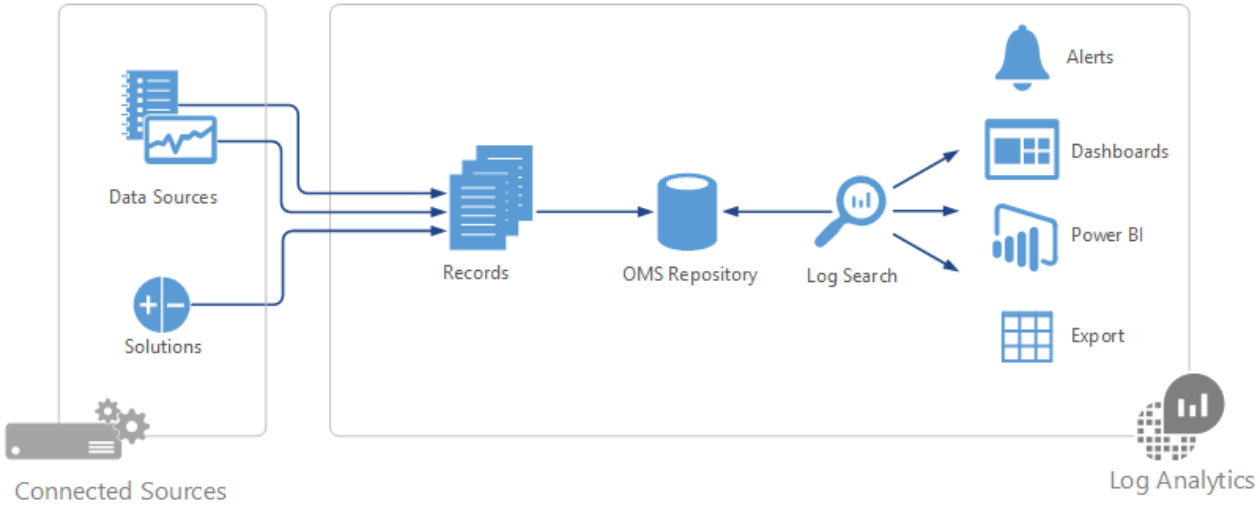


Solutions are available for a variety of functions, and additional solutions are consistently being added. You can easily browse available solutions and add them to your OMS workspace from the Solutions Gallery or Azure Marketplace. Many will be automatically deployed and start working immediately while others may require moderate configuration.



Log Analytics components

At the center of Log Analytics is the OMS repository which is hosted in the Azure cloud. Data is collected into the repository from connected sources by configuring data sources and adding solutions to your subscription. Data sources and solutions will each create different record types that have their own set of properties but may still be analyzed together in queries to the repository. This allows you to use the same tools and methods to work with different kinds of data collected by different sources.



Connected sources are the computers and other resources that generate data collected by Log Analytics. This can include agents installed on Windows and Linux computers that connect directly or agents in a connected System Center Operations Manager management group. For Azure resources, Log Analytics collects data from Azure Monitor and Azure Diagnostics.

Data sources are the different kinds of data collected from each connected source. This includes events and performance data from Windows and Linux agents in addition to sources such as IIS logs, and custom text logs. You configure each data source that you want to collect, and the configuration is automatically delivered to each connected source.

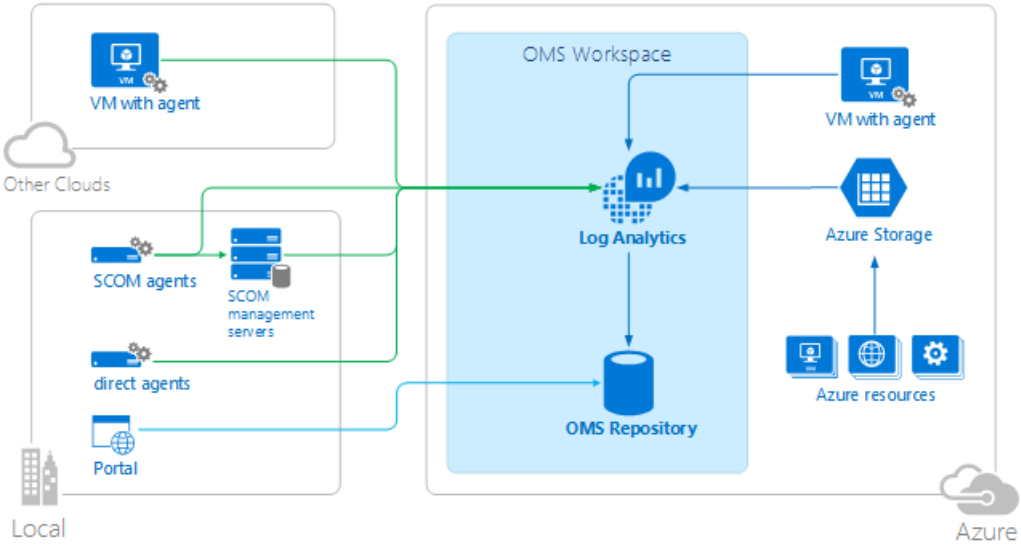
If you have custom requirements, then you can use the HTTP Data Collector API to write data to the repository from a REST API client.

Log Analytics architecture

The deployment requirements of Log Analytics are minimal since the central components are hosted in the Azure cloud. This includes the repository in addition to the services that allow you to correlate and analyze collected data. The portal can be accessed from any browser so there is no requirement for client software.

You must install agents on Windows and Linux computers, but there is no additional agent required for computers that are already members of a connected SCOM management group. SCOM agents will continue to communicate with management servers which will forward their data to Log Analytics. Some solutions though will require agents to communicate directly with Log Analytics. The documentation for each solution will specify its communication requirements.

When you sign up for Log Analytics, you will create an OMS workspace. You can think of the workspace as a unique Log Analytics environment with its own data repository, data sources, and solutions. You may create multiple workspaces in your subscription to support multiple environments such as production and test.



Next steps

- Sign up for a free Log Analytics account to test in your own environment.
- View the different Data Sources available to collect data into the OMS repository.
- Browse the available solutions in the Solutions Gallery to add functionality to Log Analytics.

Microsoft monitoring product comparison

1/17/2017 • 11 min to read • Edit Online

This article provides a comparison between System Center Operations Manager (SCOM) and Log Analytics in Operations Management Suite (OMS) in terms of their architecture, the logic of how they monitor resources, and how they perform analysis of the data they collect. This is to give you a fundamental understanding of their differences and relative strengths.

Basic Architecture

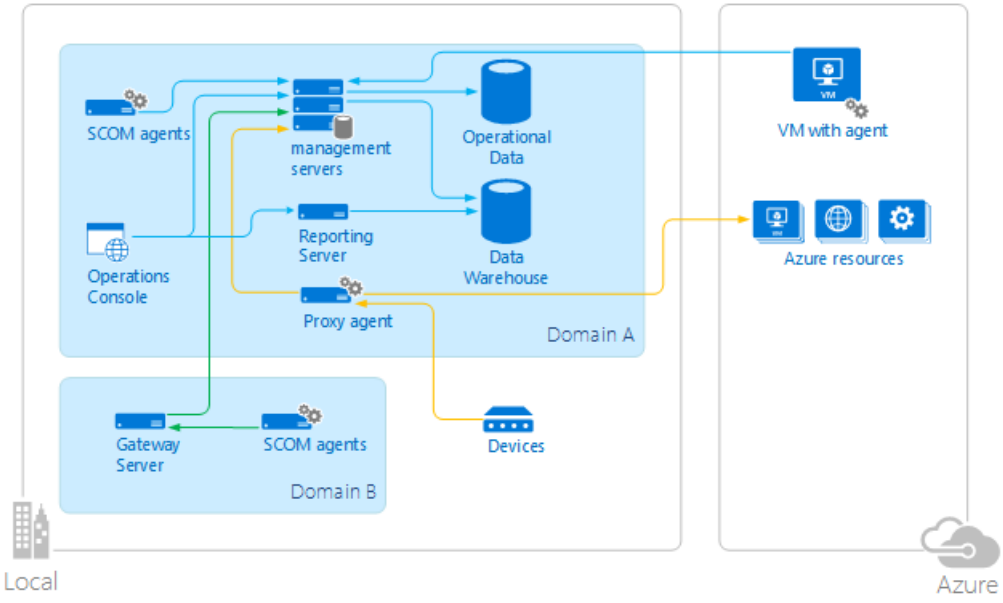
System Center Operations Manager

All SCOM components are installed in your data center. Agents are installed on Windows and Linux machines that are managed by SCOM. Agents connect to Management Servers which communicate with the SCOM database and data warehouse. Agents rely on domain authentication to connect to management servers. Those outside of a trusted domain can perform certificate authentication or connect to a Gateway Server.

SCOM requires two SQL databases, one for operational data and another data warehouse to support reporting and data analysis. A Reporting Server runs SQL Reporting Services to report on data from the data warehouse.

SCOM can monitor cloud resources using management packs for products such as Azure, Office 365, and AWS. These management packs use one or more local agents as proxies for discovering cloud resources and running workflows to measure their performance and availability. Proxy agents are also used to monitor network devices and other external resources.

The Operations Console is a Windows application that connects to one of the management servers and allows the administrator to view and analyze collected data and configure the SCOM environment . A web-based console can be hosted on any IIS server and provides data analysis through a browser.



Log Analytics

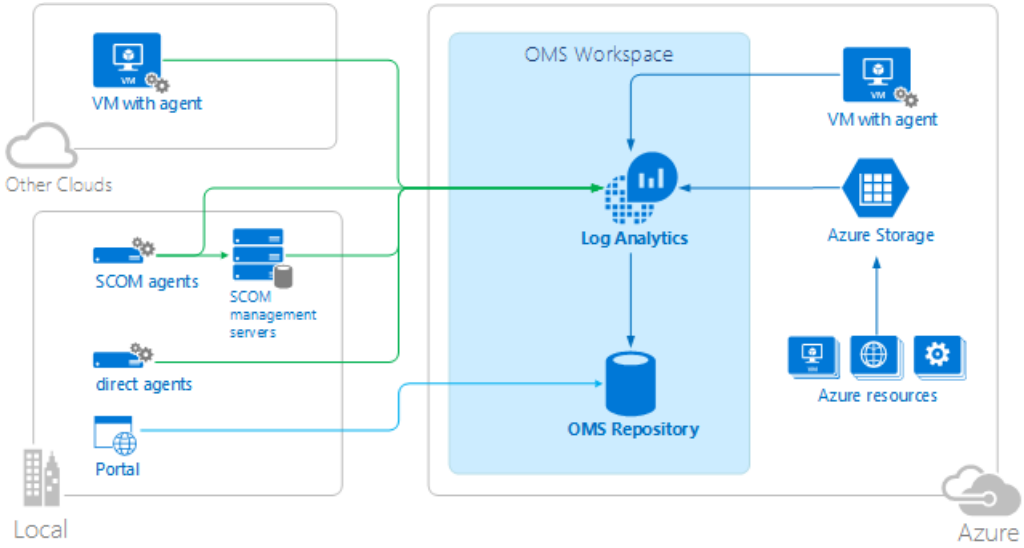
Most OMS components are in the Azure cloud so you can deploy and manage it with minimal cost and administrative effort. All data collected by Log Analytics is stored in the OMS repository.

Log Analytics can collect data from one of three sources:

- Physical and virtual machines running Windows and the Microsoft Monitoring Agent (MMA) or Linux and the

Operations Management Suite Agent for Linux. These machines can be on-premises or virtual machines in Azure or another cloud.

- An Azure Storage account with Azure Diagnostics data collected by Azure worker role, web role, or virtual machine.
- Connection to a SCOM management group. In this configuration, the agents communicate with SCOM management servers which deliver the data to the SCOM database where it is then delivered to the OMS data store. Administrators analyze collected data and configure Log Analytics with the OMS portal which is hosted in Azure and can be accessed from any browser. Mobile apps to access this data are available for the standard platforms.



Integrating SCOM and Log Analytics

When SCOM is used as a data source for Log Analytics you can leverage the features of both products in a hybrid monitoring environment. You can configure existing SCOM agents through the Operations Console to be managed by OMS, in addition to continuing to run management packs from SCOM.
Data from a connected SCOM management group is delivered to Log Analytics using one of four methods:

- Events and performance data are collected by the agent and delivered to SCOM. Management servers in SCOM then deliver the data to Log Analytics.
- Some events such as IIS logs and security events continue to be delivered directly to Log Analytics from the agent.
- Some solutions will deliver additional software to the agent or require that software be installed to collect additional data. This data will typically be sent directly to Log Analytics.
- Some solutions will collect data directly from SCOM management servers that does not originate from the agent. For example, the Alert Management solution collects alerts from SCOM after they have been created.

Monitoring Logic

SCOM and Log Analytics work with similar data collected from agents but have fundamental differences in how they define and implement their logic for data collection and how they analyze the data that they collect.

Operations Manager

Monitoring logic for SCOM is implemented in management packs which contain logic for discovering components to monitor, measuring the health of those components, and for collecting data to analyze. Monitoring data could be as simple as collecting an event or performance counter, or it could use complex logic implemented in a script. Management packs that include complete monitoring are available for a variety of Microsoft and third party applications in addition to hardware and network devices. You can author your own management packs for custom applications.

Management packs contain multiple workflows that each performs some distinct monitoring function such as sampling a performance counter, checking the state of a service, or running a script. Each workflow runs independently and defines its own results such as which database it will write to and whether it will generate an alert.

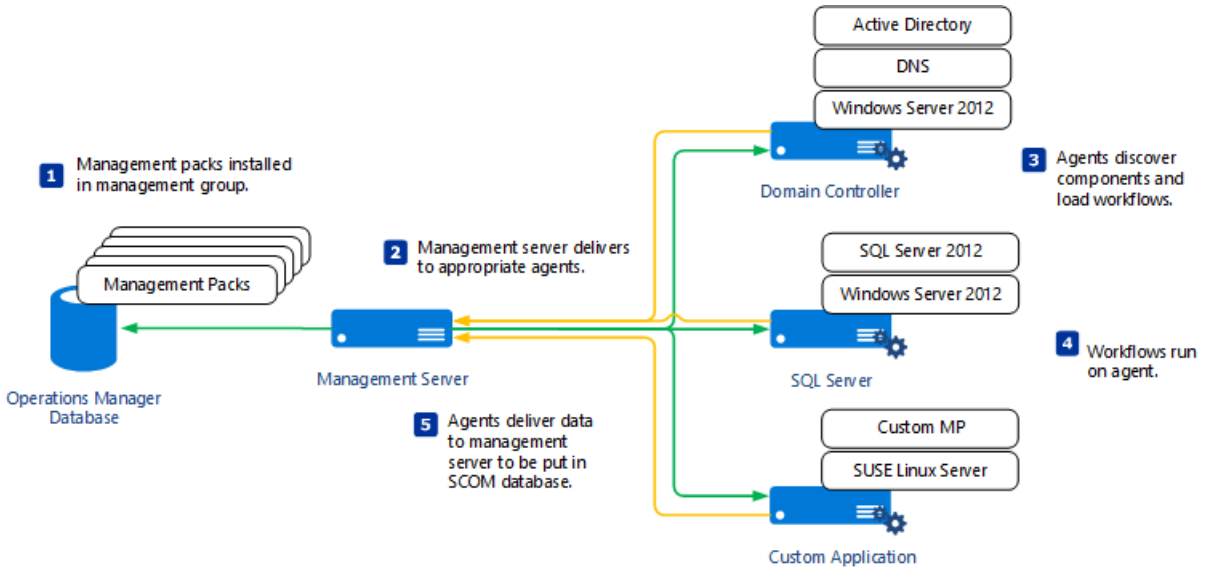
You can override details of workflow such as the frequency they run, the threshold where they consider an error, and the severity of the alert they generate. You can also provide additional functionality by adding your own workflows.

Override-controlled parameters:

Override	Parameter Name	Parameter	Default	Override	Effective Value	Change Status
☐	Alert severity	Enumeration	Critical	Critical	Critical	[No change]
☐	Auto-Resolve Alert	Boolean	True	True	True	[No change]
☑	CPU Percentage Utilization Threshold	Integer	95	80	95	[Added]
☑	CPU Queue Length Threshold	Integer	15	10	15	[Added]
☐	Enabled	Boolean	True	True	True	[No change]
☐	Generates Alert	Boolean	True	True	True	[No change]
☐	Interval seconds	Integer	900	900	900	[No change]
☐	Number of Samples	Integer	3	3	3	[No change]

Management packs are installed in the Operations Manager database and automatically distributed to agents by management servers. Each agent will automatically download management packs and load workflows relevant to the applications they have installed. Data collected by the agent is delivered back to the management server for insertion into the SCOM database and data warehouse. The Operations Console allows you to view and analyze this data through custom views, dashboards, and reports included in the management pack.

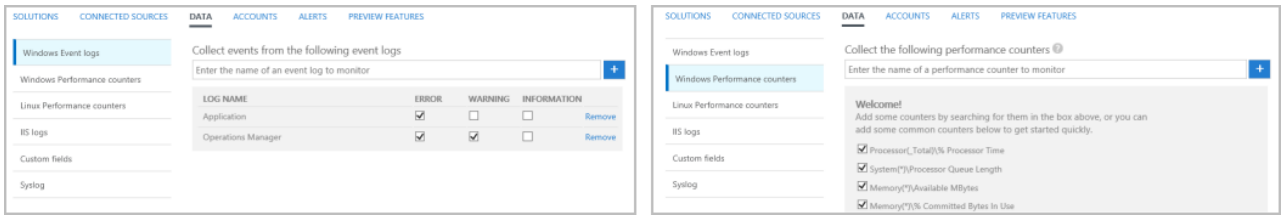
The distribution of management packs is illustrated in the following diagram.



Log Analytics

Event and Performance Collection

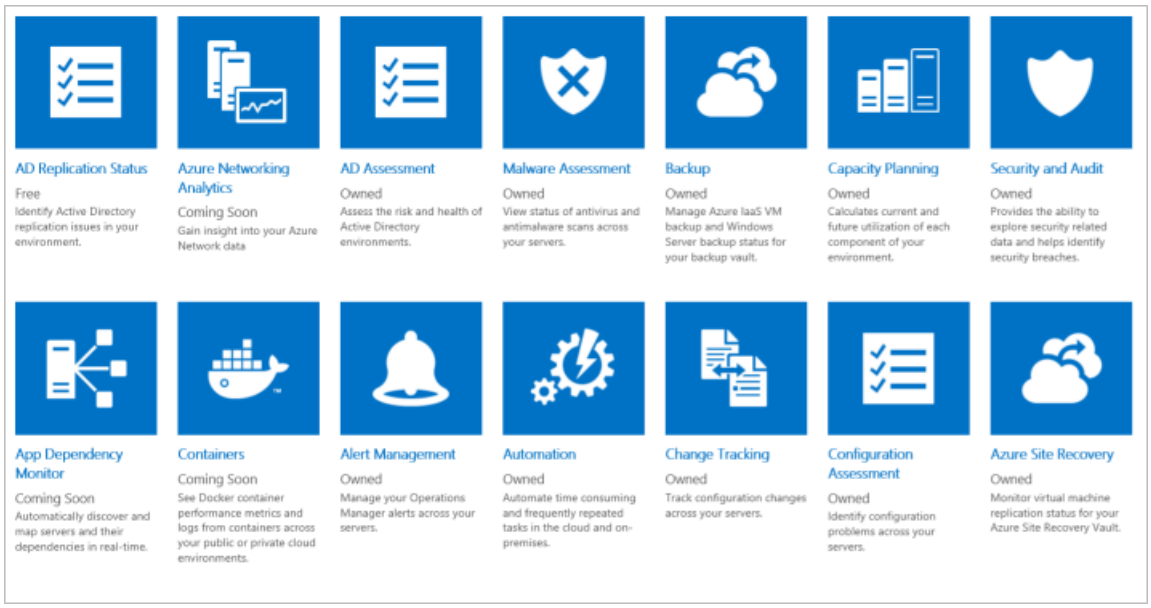
Log Analytics collects events and performance counters from agent systems using sources such as Windows event log, IIS logs, and Syslog. You can define criteria for which data is collected through the Log Analytics portal and then create Log Queries to analyze the collected data. A set of standard criteria is defined when you create your OMS workspace, and you can define additional data for particular applications.



While SCOM has many detailed workflows that typically define specific criteria for data and the action that should be performed in response, Log Analytics has more general criteria for data collection. Log queries and solutions provide more targeted criteria for analyzing and acting on specific data in the cloud after it's been collected.

Solutions

Solutions provide additional logic for data collection and analysis. You can select solutions to add to your OMS subscription from the Solution Gallery.

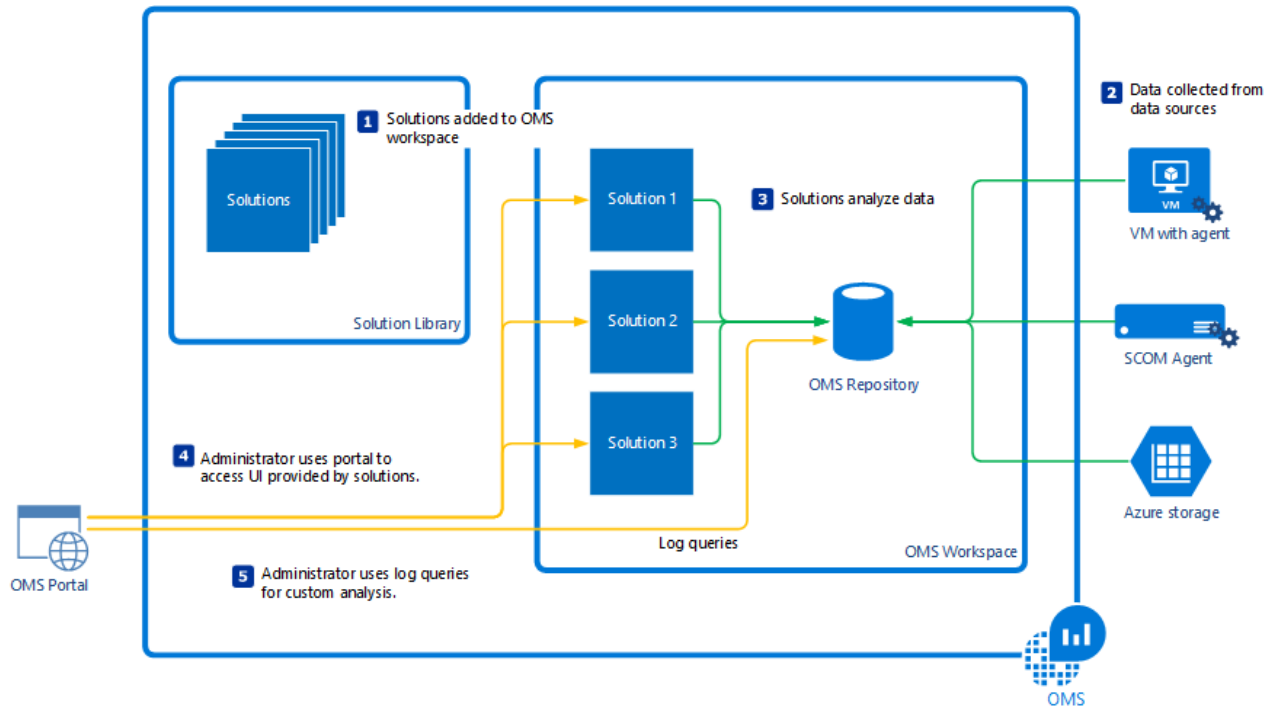


Solutions primarily run in the cloud providing analysis of events and performance counters collected in the OMS repository. They may also define additional data to be collected that can be analyzed with Log Queries or by additional user interface provided by the solution in the OMS dashboard.

For example, the Change Tracking solution detects configuration changes on agent systems and writes events to the OMS repository that can be analyzed with several graphical views that summarize detected changes. You can drill down from the summarized view into log queries that display the detailed data collected by the solution.

While you can select which solutions you add to your subscription, you don't currently have the ability to create your own solutions. You can select the events and performance counters to collect and create custom views based on your own log queries.

The monitoring logic for Log Analytics is summarized in the following diagram.

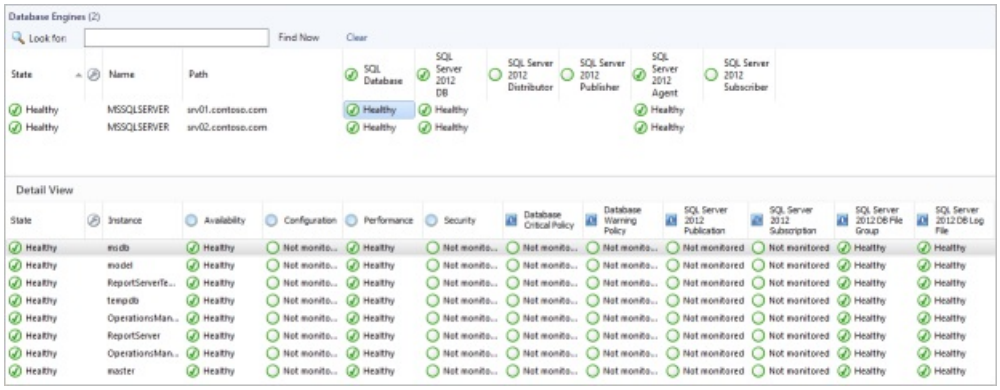


Health Monitoring

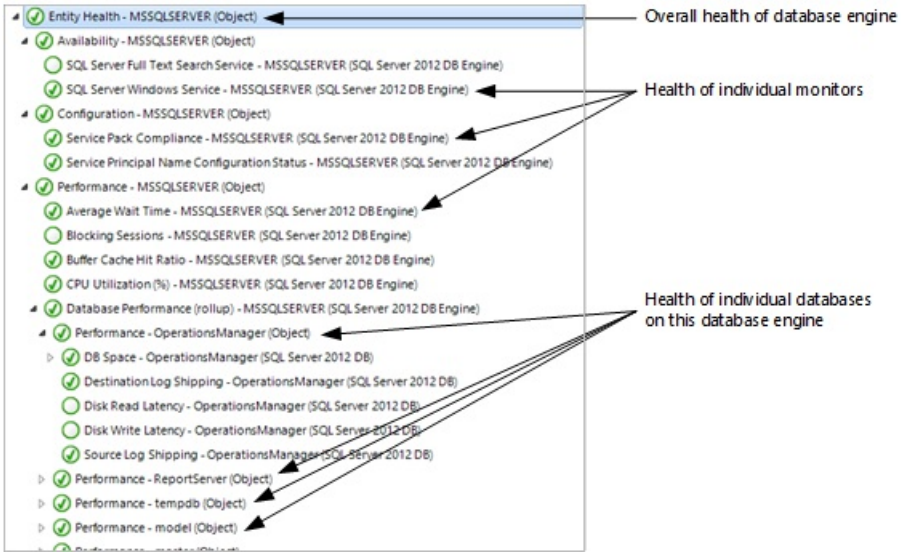
Operations Manager

SCOM can model the different components of an application and provide a real-time health for each. This allows you to not only view detected errors and performance over time but also to validate the actual health of an application or system and each of its components at any given time. Because it understands the time periods that an application is available, the health engine in SCOM also supports Service Level Agreements (SLA) which analyze and report on the availability of an application over time.

For example, the view below shows the real-time health of SQL database engines monitored by SCOM. The health of each of the databases for one of the database engines is shown on the bottom half of the view.

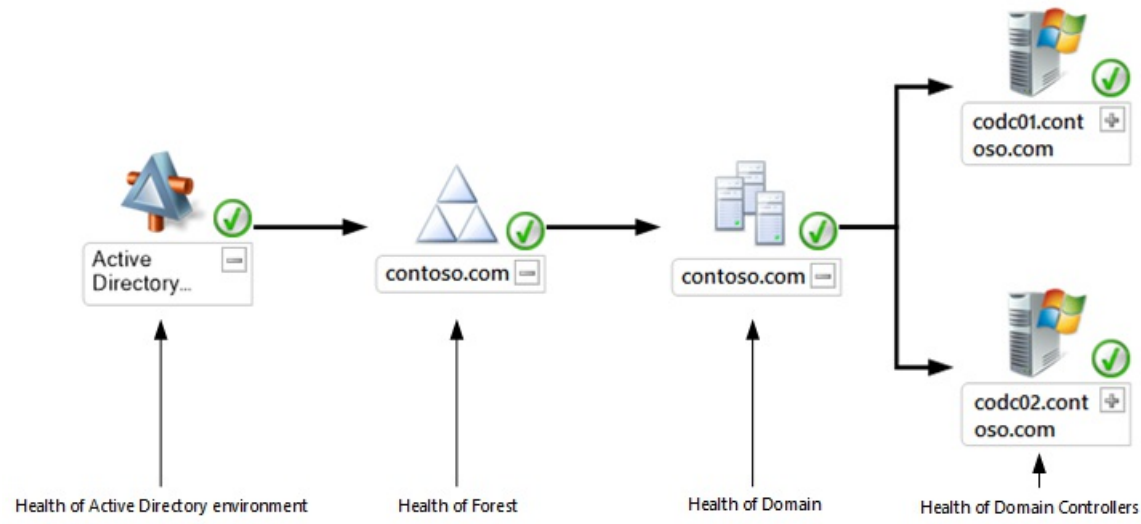


The Health Explorer for one of the database engines is shown below with the monitors that are used to determine its overall health. These monitors are defined in the SQL management pack and run against all SQL database engines discovered by SCOM.



Components on multiple systems can be combined to measure the health of a distributed application. This can be particularly useful for line of business applications that include multiple distributed components. You can create a model that measures the health of each component that rollup into availability for the application.

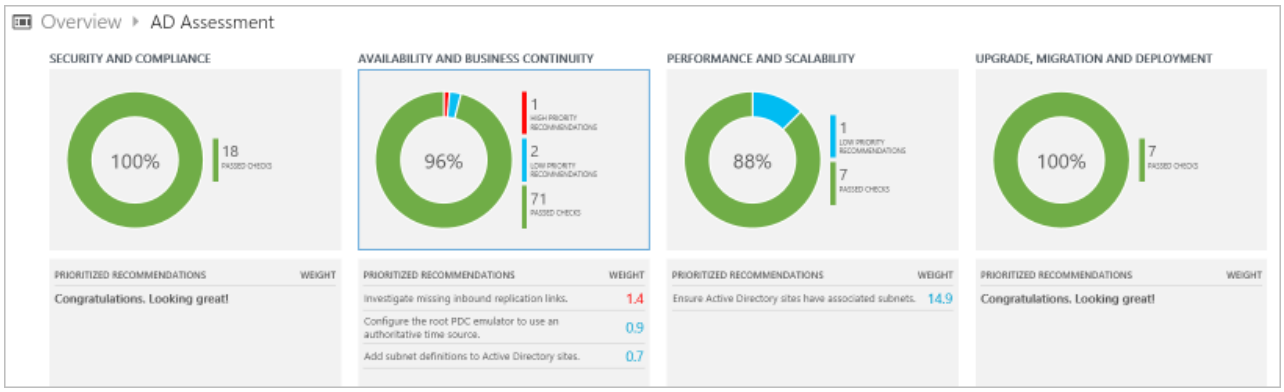
Active Directory is an example of one management pack that provides a model to analyze its distributed components. The sample diagram below shows the health of the overall environment and the relationship between forests, domains, and domain controllers. Each of these components includes subcomponents and multiple monitors similar to the SQL example above.



Log Analytics

OMS does not include a common engine to model applications or measure their real-time health. Individual solutions may assess the overall health of particular services based on collected data, and they may install custom logic on the agent to perform real-time analysis. Because solutions run in the cloud with access to the OMS repository, they can often provide deeper analysis than is typically performed by management packs.

For example, the AD Assessment and SQL Assessment solutions analyze collected data and provide a rating for different aspects of the environment. It includes recommendations for improvements that can be made to improve the availability and performance of the environment.



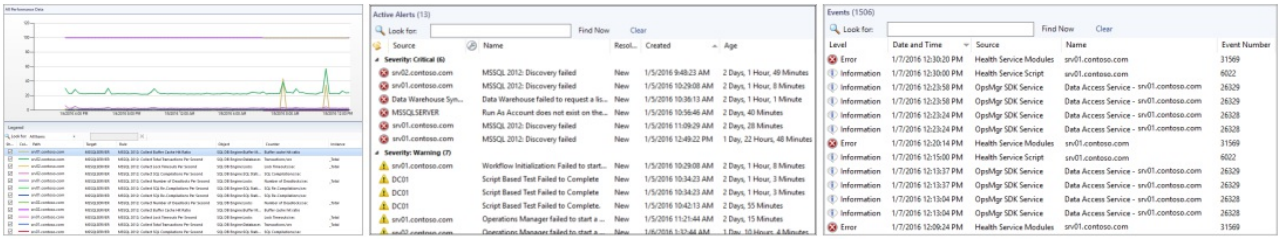
Data Analysis

SCOM and Log Analytics each provide different features to analyze collected data. SCOM has Views and Dashboards in the Operations Console for analyzing recent data in a variety of formats and reports for presenting data from the data warehouse in tabular form. Log Analytics provides a complete log query language and interface for analyzing data in the OMS repository. When SCOM is used as a data source for Log Analytics, the repository includes data collected by SCOM so the Log Analytics tools can be used to analyze data from both systems.

Operations Manager

Views

Views in the Operations Console allow you to view different data types collected by SCOM in different formats, typically tabular for events, alerts, and state data, and line graphs for performance data. Views perform minimal analysis or consolidation of the data but do allow you to filter according to particular criteria.

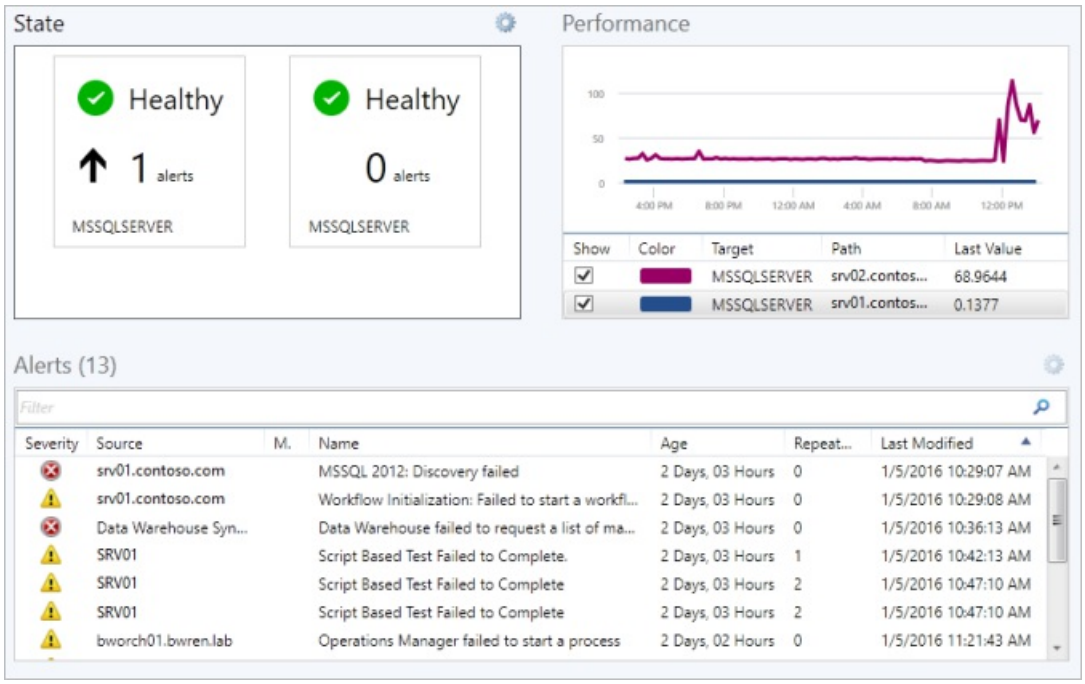


Management packs will typically provide multiple views supporting the application or system that it monitors. This may include state views for the different objects that the management pack discovers, alert views for detected issues, and performance views for counters.

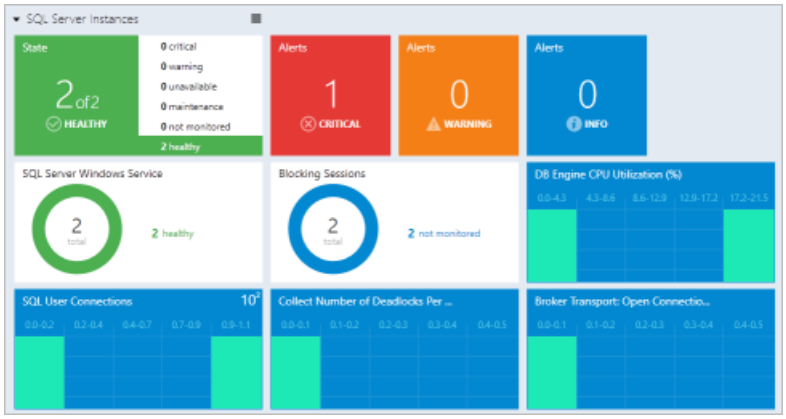
Views are particularly suitable for analyzing the current state of the environment including open alerts and the health state of monitored systems and objects. You can drill down to detailed event or performance data supporting a particular alert in order to diagnose its root cause. Similarly, you can view the performance and health of different components of an application to assess its current health.

Dashboards

Dashboards in the Operations Console primarily work with the same data as views but are more customizable and can include richer visualizations. A set of standard dashboards are available that you can easily customize for your own purposes. You can also use a PowerShell widget which can display data returned from a PowerShell query.



Developers have the ability to add custom components to dashboards they include in their management packs. These may be highly specialized to a particular application such as the dashboard in the SQL management pack shown below. This dashboard can also be used as a template for custom versions.

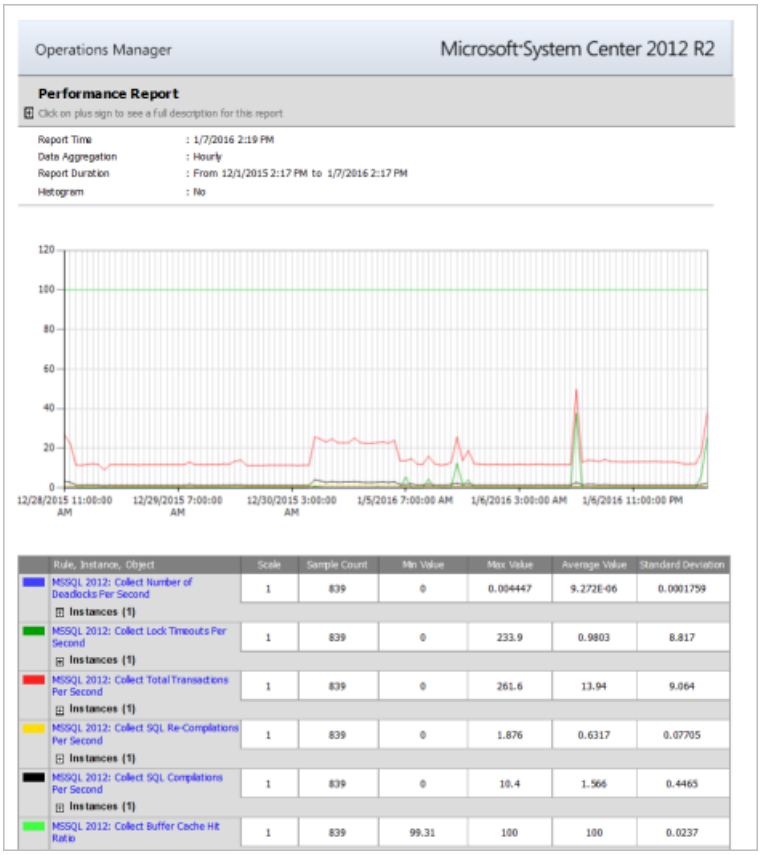


Reports

Reports in SCOM analyze data from the data warehouse in tabular form. They can be printed and scheduled for automated delivery in different file formats including PDF, CSV, and Word. Reports work with data from the data warehouse so they are especially suitable for analysis of long term trends.

Management packs will typically provide custom reports for a particular application. You can also select from a library of generic reports that you can customize for your own applications or for performing ad hoc analysis.

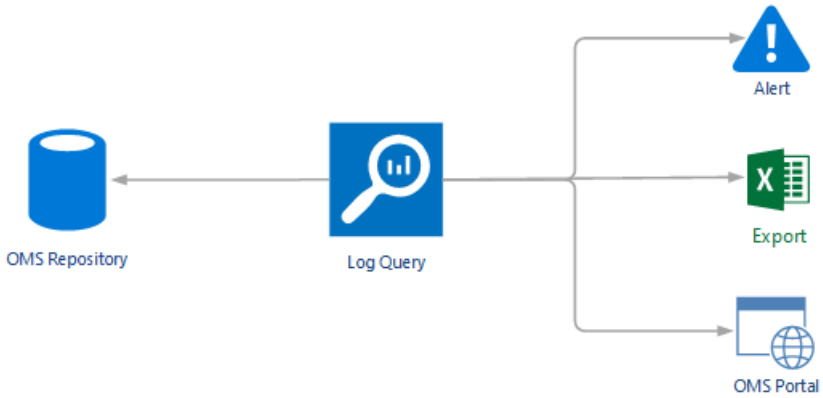
Following is a sample performance report showing data collected by the Active Directory Management Pack.



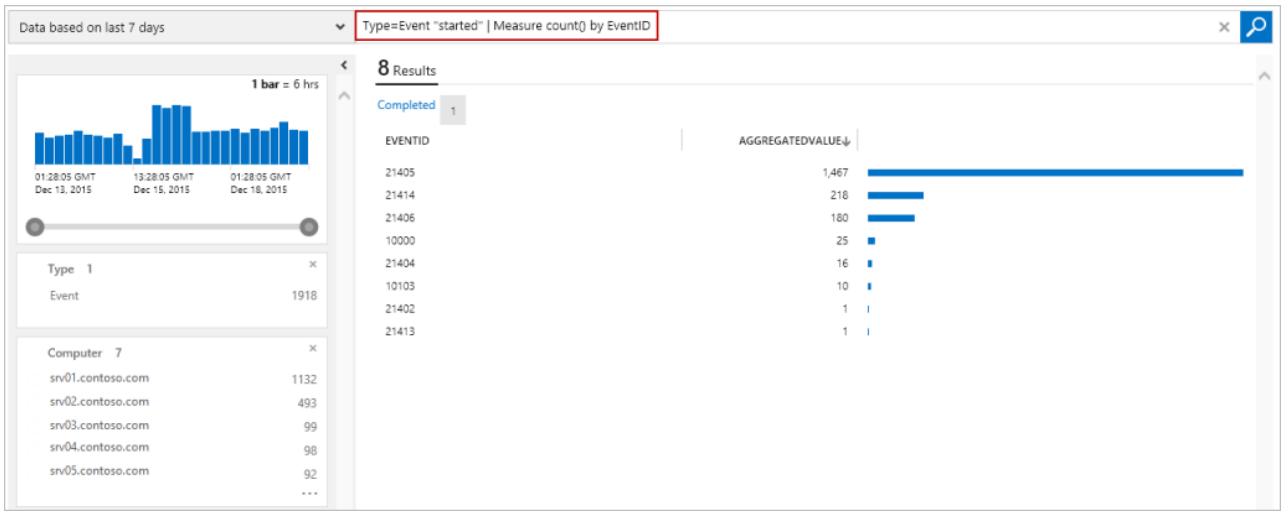
Log Analytics

Log Analytics has a query language that you can use to perform analysis across data from multiple applications without the need to create a custom view or report. Because OMS is implemented in the cloud, performance of queries and data analysis are not subject to any hardware limitations and can quickly analyze queries including millions of records.

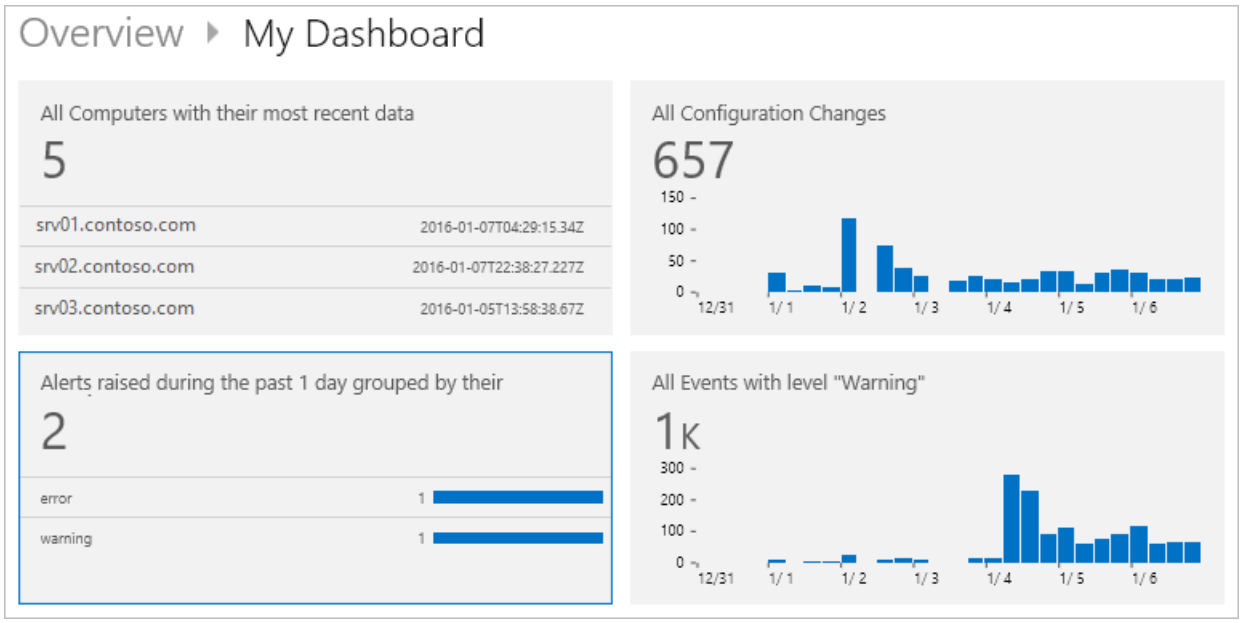
Queries in Log Analytics are also the basis of other functionality. You can save a query, export its results to Excel, or have it automatically run at regular intervals and generate an alert if its results match particular criteria.



Below is an example of a Log Analytics query. In this example all events with “started” in the name are returned and grouped by event ID. The user simply provides the query, and Log Analytics dynamically generates the user interface to perform the analysis. Selecting any item in the list will return the detailed event data.



In addition to providing ad hoc analysis, queries in Log Analytics can be saved for future use and also added to your OMS dashboard as shown in the following example.



Next Steps

- Deploy System Center Operations Manager (SCOM).
- Sign up for Log Analytics.

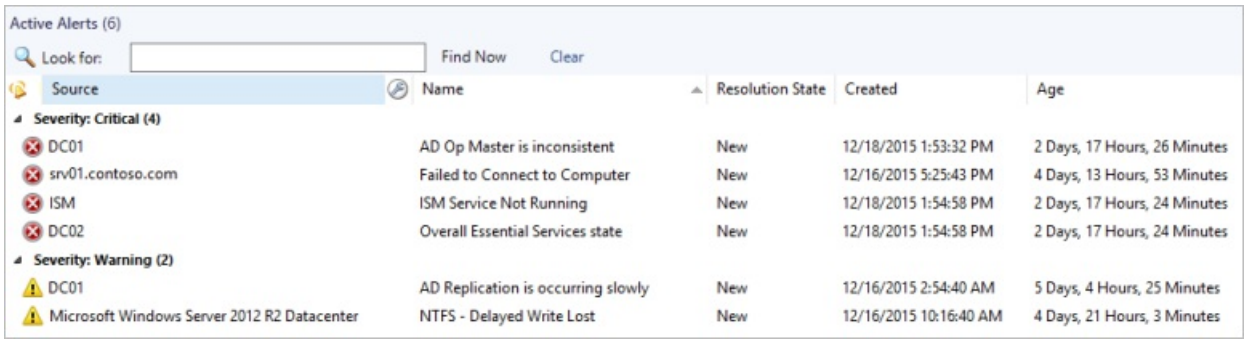
Managing alerts with Microsoft monitoring

4/12/2017 • 4 min to read • Edit Online

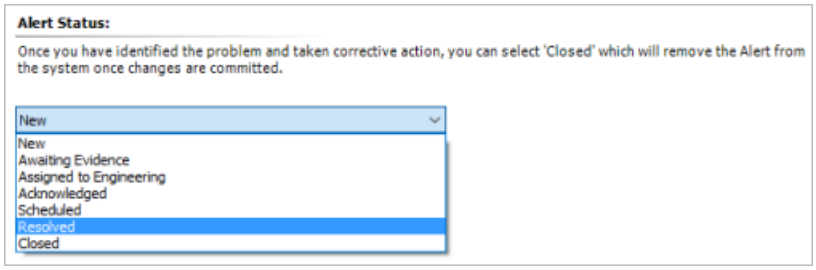
An alert indicates some issue that requires attention from an administrator. There are distinct differences between System Center Operations Manager (SCOM) and Log Analytics in Operations Management Suite (OMS) in terms of how alerts are created, how they are managed and analyzed, and how you are notified that a critical issue has been detected.

Alerts in Operations Manager

Alerts in SCOM are generated by individual rules or monitors to indicate a specific issue. A monitor can generate an alert when it enters an error state while a rule may generate an alert to indicate some critical issue that is not directly related to the health of a managed object. Management packs include a variety of workflows that create alerts for the application or service that they manage. Part of the process of configuring a new management pack is tuning it to ensure that you don't receive excessive alerts for issues that you don't consider critical.



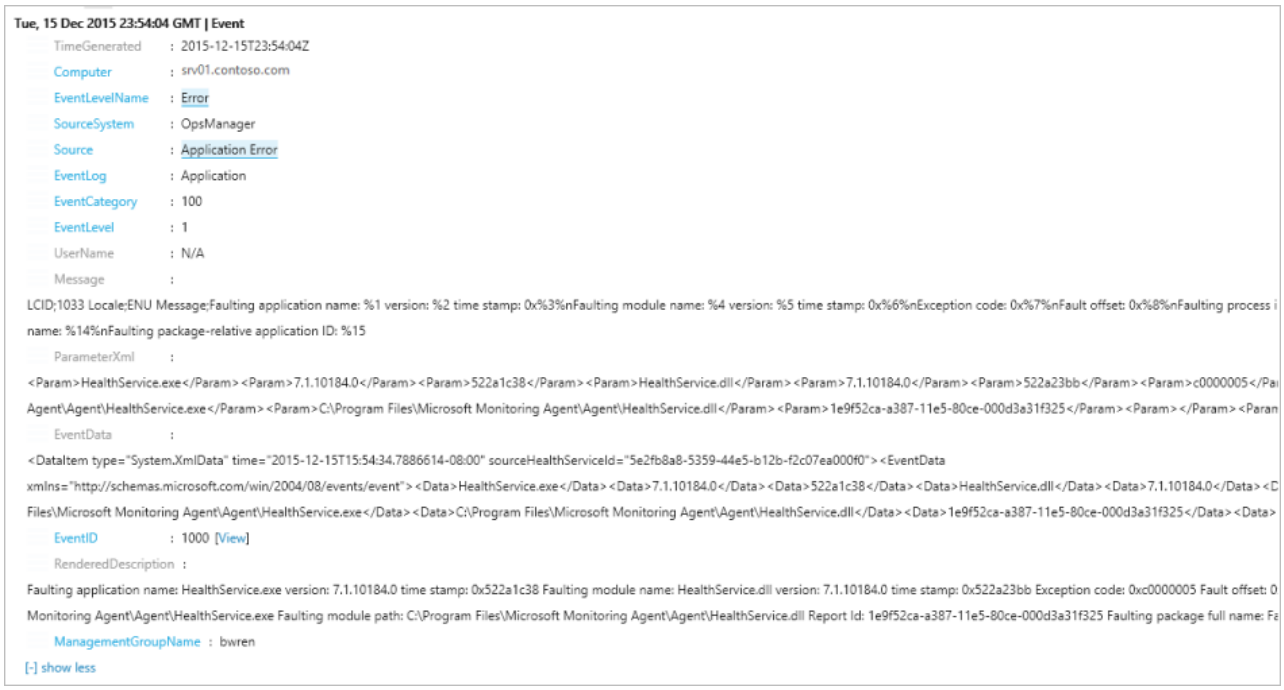
SCOM provides complete alert management with alerts having a status that can be changed by administrators as they work to resolve the issue. When the issue has been resolved, the administrator sets the alert to closed at which time it will no longer appear in views displaying active alerts. Alerts that are generated from monitors can be automatically resolved when the monitor returns to a healthy state.



Alerts in Log Analytics

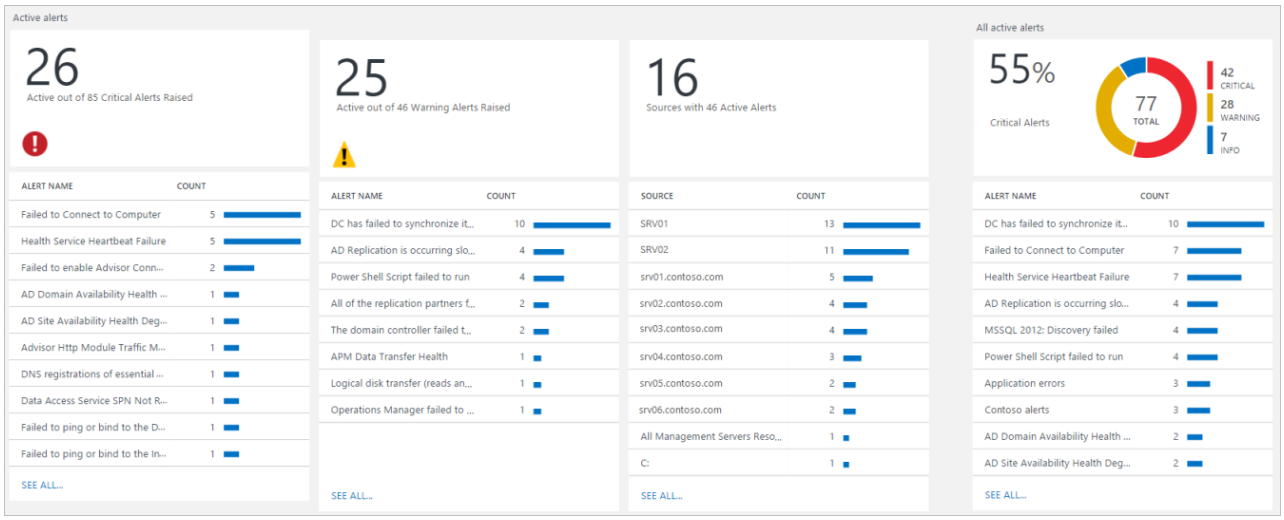
An alert in Log Analytics is created from a log query that is automatically run at regular intervals. You can create an alert rule from any log query. If the query returns results that match the criteria that you specify, then an alert is created. This could be a specific query that creates an alert if a particular event is detected, or you could use a more general query that looks for any error event related to a particular application.

Log Analytics alerts are written to the OMS repository as an event and can be retrieved with a log query. They do not have a status like SCOM events so that you can indicate when the issue has been resolved.



When SCOM is used as a data source for Log Analytics, SCOM alerts are written to the OMS repository as they are created and modified.

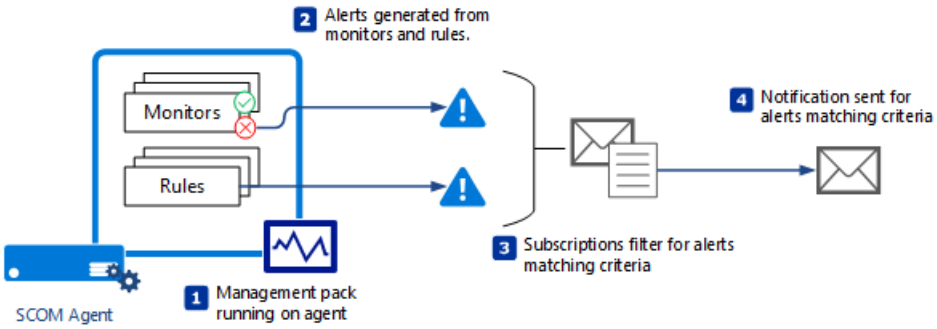
The Alert Management solution provides a summary of active alerts and several common queries to retrieve different sets of alerts. This provides you with more effective analysis of your alerts than a report in SCOM. You can drill down on from the summaries to detailed data and create ad hoc queries to retrieve different sets of alerts.



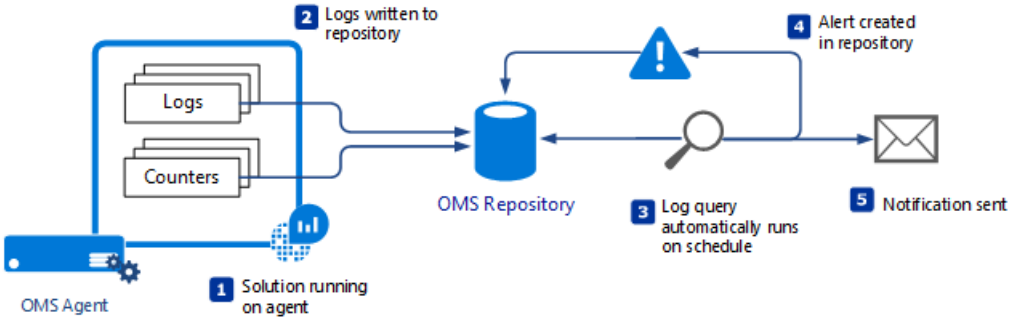
Notifications

Notifications in SCOM send you a mail or text in response to alerts that match particular criteria. You can create different notification subscriptions that have different people notified depending on such criteria as the object being monitored, the severity of the alert, the kind of problem that detected, or the time of day.

Few subscriptions can be used to implement a complete notification strategy for a large number of management packs.



Log Analytics can notify you through mail that an alert has been created by setting an email notification action on each alert rule. It does not have the ability of SCOM the subscribe to multiple alerts with a single rule. You also need to create your own alert rules since OMS does not provide any preconfigured.



You can't completely manage SCOM alerts in Log Analytics though since you can only modify them in the Operations Console. Log Analytics is useful as part of an alert management process though for providing analysis tools that SCOM alone doesn't have.

Alert Remediation

Remediation refers to an attempt to automatically correct the problem identified by an alert.

SCOM allows you to run Diagnostics and Recoveries in response to a monitor entering an unhealthy state. This

happens simultaneous to the monitor creating the alert. Diagnostics and recoveries are typically implemented as a script that runs on the agent. A diagnostic attempts to gather more information about the detected issue while a recovery attempts to correct the problem.

Log Analytics allows you to start an Azure Automation runbook or call a webhook in response to a Log Analytics alert. Runbooks can contain complex logic implemented in PowerShell. The script runs in Azure and can access any Azure resources or external resources available from the cloud. Azure Automation does have the ability to execute runbooks on a server in your local datacenter, but this feature is not currently available when starting the runbook in response to Log Analytics alerts.

Both recoveries in SCOM and runbooks in OMS can contain PowerShell scripts, but recoveries are more difficult to create and manage because they must be contained within a management pack. Runbooks are stored in Azure Automation which provides features for authoring, testing, and managing runbooks.

If you use SCOM as a data source for Log Analytics, you could create a Log Analytics alert using a log query to retrieve SCOM alerts stored in the OMS repository. This would allow you to run an Azure Automation runbook in response to a SCOM alert. Of course, since the runbook will run in Azure, this would not be a viable strategy for recoveries of on-premises issues.

Next steps

- Learn the details of alerts in System Center Operations Manager (SCOM).

Azure Automation overview

1/17/2017 • 6 min to read • Edit Online

Microsoft Azure Automation provides a way for users to automate the manual, long-running, error-prone, and frequently repeated tasks that are commonly performed in a cloud and enterprise environment. It saves time and increases the reliability of regular administrative tasks and even schedules them to be automatically performed at regular intervals. You can automate processes using runbooks or automate configuration management using Desired State Configuration. This article provides brief overview of Azure Automation and answers some common questions. You can refer to other articles in this library for more detailed information on the different topics.

Automating processes with runbooks

A runbook is a set of tasks that perform some automated process in Azure Automation. It may be a simple process such as starting a virtual machine and creating a log entry, or you may have a complex runbook that combines other smaller runbooks to perform a complex process across multiple resources or even multiple clouds and on premise environments.

For example, you might have an existing manual process for truncating a SQL database if it's approaching maximum size that includes multiple steps such as connecting to the server, connecting to the database, get the current size of database, check if threshold has exceeded and then truncate it and notify user. Instead of manually performing each of these steps, you could create a runbook that would perform all of these tasks as a single process. You would start the runbook, provide the required information such as the SQL server name, database name, and recipient e-mail and then sit back while the process completes.

What can runbooks automate?

Runbooks in Azure Automation are based on Windows PowerShell or Windows PowerShell Workflow, so they do anything that PowerShell can do. If an application or service has an API, then a runbook can work with it. If you have a PowerShell module for the application, then you can load that module into Azure Automation and include those cmdlets in your runbook. Azure Automation runbooks run in the Azure cloud and can access any cloud resources or external resources that can be accessed from the cloud. Using Hybrid Runbook Worker, runbooks can run in your local data center to manage local resources.

Getting runbooks from the community

The Runbook Gallery contains runbooks from Microsoft and the community that you can either use unchanged in your environment or customize them for your own purposes. They are also useful to as references to learn how to create your own runbooks. You can even contribute your own runbooks to the gallery that you think other users may find useful.

Creating Runbooks with Azure Automation

You can create your own runbooks from scratch or modify runbooks from the Runbook Gallery for your own requirements. There are four different runbook types that you can choose from based on your requirements and PowerShell experience. If you prefer to work directly with the PowerShell code, then you can use a PowerShell runbook or PowerShell Workflow runbook that you edit offline or with the textual editor in the Azure portal. If you prefer to edit a runbook without being exposed to the underlying code, then you can create a Graphical runbook using the graphical editor in the Azure portal.

Prefer watching to reading? Have a look at the below video from Microsoft Ignite session in May 2015. Note: While

the concepts and features discussed in this video are correct, Azure Automation has progressed a lot since this video was recorded, it now has a more extensive UI in the Azure portal, and supports additional capabilities.

Automating configuration management with Desired State Configuration

PowerShell DSC is a management platform that allows you to manage, deploy and enforce configuration for physical hosts and virtual machines using a declarative PowerShell syntax. You can define configurations on a central DSC Pull Server that target machines can automatically retrieve and apply. DSC provides a set of PowerShell cmdlets that you can use to manage configurations and resources.

Azure Automation DSC is a cloud based solution for PowerShell DSC that provides services required for enterprise environments. You can manage your DSC resources in Azure Automation and apply configurations to virtual or physical machines that retrieve them from a DSC Pull Server in the Azure cloud. It also provides reporting services that inform you of important events such as when nodes have deviated from their assigned configuration and when a new configuration has been applied.

Creating your own DSC configurations with Azure Automation

DSC configurations specify the desired state of a node. Multiple nodes can apply the same configuration to assure that they all maintain an identical state. You can create a configuration using any text editor on your local machine and then import it into Azure Automation where you can compile it and apply it nodes.

Getting modules and configurations

You can get PowerShell modules containing cmdlets that you can use in your runbooks and DSC configurations from the PowerShell Gallery. You can launch this gallery from the Azure portal and import modules directly into Azure Automation, or you can download and import them manually. You cannot install the modules directly from the Azure portal, but you can download them install them as you would any other module.

Example practical applications of Azure Automation

Following are just a few examples of what are the kinds of automation scenarios with Azure Automation.

- Create and copy virtual machines in different Azure subscriptions.
- Schedule file copies from a local machine to an Azure Blob Storage container.
- Automate security functions such as deny requests from a client when a denial of service attack is detected.
- Ensure machines continually align with configured security policy.
- Manage continuous deployment of application code across cloud and on premises infrastructure.
- Build an Active Directory forest in Azure for your lab environment.
- Truncate a table in a SQL database if DB is approaching maximum size.
- Remotely update environment settings for an Azure website.

How does Azure Automation relate to other automation tools?

Service Management Automation (SMA) is intended to automate management tasks in the private cloud. It is

installed locally in your data center as a component of Microsoft Azure Pack. SMA and Azure Automation use the same runbook format based on Windows PowerShell and Windows PowerShell Workflow, but SMA does not support graphical runbooks.

System Center 2012 Orchestrator is intended for automation of on-premises resources. It uses a different runbook format than Azure Automation and Service Management Automation and has a graphical interface to create runbooks without requiring any scripting. Its runbooks are composed of activities from Integration Packs that are written specifically for Orchestrator.

Where can I get more information?

A variety of resources are available for you to learn more about Azure Automation and creating your own runbooks.

- **Azure Automation Library** is where you are right now. The articles in this library provide complete documentation on the configuration and administration of Azure Automation and for authoring your own runbooks.
- Azure PowerShell cmdlets provides information for automating Azure operations using Windows PowerShell. Runbooks use these cmdlets to work with Azure resources.
- Management Blog provides the latest information on Azure Automation and other management technologies from Microsoft. You should subscribe to this blog to stay up to date with the latest from the Azure Automation team.
- Automation Forum allows you to post questions about Azure Automation to be addressed by Microsoft and the Automation community.
- Azure Automation Cmdlets provides information for automating administration tasks. It contains cmdlets to manage Automation accounts, assets, runbooks, DSC.

Can I provide feedback?

Please give us feedback! If you are looking for an Azure Automation runbook solution or an integration module, post a Script Request on Script Center. If you have feedback or feature requests for Azure Automation, post them on User Voice. Thanks!

Overview of the features in Azure Backup

5/4/2017 • 20 min to read • Edit Online

Azure Backup is the Azure-based service you can use 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 is reliable, secure, and cost-competitive. Azure Backup offers multiple components that you download and deploy on the appropriate computer, server, or in the cloud. The component, or agent, that you deploy depends on what you want to protect. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Backup vault in Azure. See the Azure Backup components table (later in this article) for information about which component to use to protect specific data, applications, or workloads.

Watch a video overview of Azure Backup

Why use Azure Backup?

Traditional backup solutions have evolved to treat the cloud as an endpoint, or static storage destination, similar to disks or tape. While this approach is simple, it is limited and doesn't take full advantage of an underlying cloud platform, which translates to an expensive, inefficient solution. Other solutions are expensive because you end up paying for the wrong type of storage, or storage that you don't need. Other solutions are often inefficient because they don't offer you the type or amount of storage you need, or administrative tasks require too much time. In contrast, Azure Backup delivers these key benefits:

Automatic storage management - Hybrid environments often require heterogeneous storage - some on-premises and some in the cloud. With Azure Backup, there is no cost for using on-premises storage devices. Azure Backup automatically allocates and manages backup storage, and it uses a pay-as-you-use model. Pay-as-you-use means that you only pay for the storage that you consume. For more information, see the Azure pricing article.

Unlimited scaling - Azure Backup uses the underlying power and unlimited scale of the Azure cloud to deliver high-availability - with no maintenance or monitoring overhead. You can set up alerts to provide information about events, but you don't need to worry about high-availability for your data in the cloud.

Multiple storage options - An aspect of high-availability is storage replication. Azure Backup offers two types of replication: locally redundant storage and geo-redundant storage. Choose the backup storage option based on need:

- Locally redundant storage (LRS) replicates your data three times (it creates three copies of your data) in a paired datacenter in the same region. LRS is a low-cost option for protecting your data from local hardware failures.
- Geo-redundant storage (GRS) replicates your data to a secondary region (hundreds of miles away from the primary location of the source data). GRS costs more than LRS, but GRS provides a higher level of durability for your data, even if there is a regional outage.

Unlimited data transfer - Azure Backup does not limit the amount of inbound or outbound data you transfer. Azure Backup also does not charge for the data that is transferred. However, if you use the Azure Import/Export service to import large amounts of data, there is a cost associated with inbound data. For more information about this cost, see Offline-backup workflow in Azure Backup. Outbound data refers to data transferred from a Backup vault during a restore operation.

Data encryption - Data encryption allows for secure transmission and storage of your data in the public cloud. You store the encryption passphrase locally, and it is never transmitted or stored in Azure. If it is necessary to restore any of the data, only you have encryption passphrase, or key.

Application-consistent backup - Whether backing up a file server, virtual machine, or SQL database, you need to know that a recovery point has all required data to restore the backup copy. Azure Backup provides application-consistent backups, which ensured additional fixes are not needed to restore the data. Restoring application consistent data reduces the restoration time, allowing you to quickly return to a running state.

Long-term retention - Instead of switching backup copies from disk to tape and moving the tape to an off-site location, you can use Azure for short-term and long-term retention. Azure doesn't limit the length of time data remains in a Backup or Recovery Services vault. You can keep data in a vault for as long as you like. Azure Backup has a limit of 9999 recovery points per protected instance. See the Backup and retention section in this article for an explanation of how this limit may impact your backup needs.

Which Azure Backup components should I use?

If you aren't sure which Azure Backup component works for your needs, see the following table for information about what you can protect with each component. The Azure portal provides a wizard, which is built into the portal, to guide you through choosing the component to download and deploy. The wizard, which is part of the Recovery Services vault creation, leads you through the steps for selecting a backup goal, and choosing the data or application to protect.

COMPONENT	BENEFITS	LIMITS	WHAT IS PROTECTED?	WHERE ARE BACKUPS STORED?
Azure Backup (MARS) agent	• Back up files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure) • No separate backup server required.	• Backup 3x per day • Not application aware; file, folder, and volume-level restore only, • No support for Linux.	• Files, • Folders	Azure Backup vault
System Center DPM	• Application-aware snapshots (VSS) • Full flexibility for when to take backups • Recovery granularity (all) • Can use Azure Backup vault • Linux support on Hyper-V and VMware VMs • Back up and restore VMware VMs using DPM 2012 R2	Cannot back up Oracle workload.	• Files, • Folders, • Volumes, • VMs, • Applications, • Workloads	• Azure Backup vault, • Locally attached disk, • Tape (on-premises only)

COMPONENT	BENEFITS	LIMITS	WHAT IS PROTECTED?	WHERE ARE BACKUPS STORED?
Azure Backup Server	• App aware snapshots (VSS) • Full flexibility for when to take backups • Recovery granularity (all) • Can use Azure Backup vault • Linux support on Hyper-V and VMware VMs • Back up and restore VMware VMs • Does not require a System Center license	• Cannot back up Oracle workload. • Always requires live Azure subscription • No support for tape backup	• Files, • Folders, • Volumes, • VMs, • Applications, • Workloads	• Azure Backup vault, • Locally attached disk
Azure IaaS VM Backup	• Native backups for Windows/Linux • No specific agent installation required • Fabric-level backup with no backup infrastructure needed	• Back up VMs once-a-day • Restore VMs only at disk level • Cannot back up on-premises	• VMs, • All disks (using PowerShell)	Azure Backup vault

What are the deployment scenarios for each component?

COMPONENT	CAN BE DEPLOYED IN AZURE?	CAN BE DEPLOYED ON-PREMISES?	TARGET STORAGE SUPPORTED
Azure Backup (MARS) agent	**Yes** The Azure Backup agent can be deployed on any Windows Server VM that runs in Azure.	**Yes** The Backup agent can be deployed on any Windows Server VM or physical machine.	Azure Backup vault
System Center DPM	**Yes** Learn more about how to protect workloads in Azure by using System Center DPM.	**Yes** Learn more about how to protect workloads and VMs in your datacenter.	Locally attached disk, Azure Backup vault, tape (on-premises only)
Azure Backup Server	**Yes** Learn more about how to protect workloads in Azure by using Azure Backup Server.	**Yes** Learn more about how to protect workloads in Azure by using Azure Backup Server.	Locally attached disk, Azure Backup vault

COMPONENT	CAN BE DEPLOYED IN AZURE?	CAN BE DEPLOYED ON-PREMISES?	TARGET STORAGE SUPPORTED
Azure IaaS VM Backup	**Yes** Part of Azure fabric Specialized for backup of Azure infrastructure as a service (IaaS) virtual machines.	**No** Use System Center DPM to back up virtual machines in your datacenter.	Azure Backup vault

Which applications and workloads can be backed up?

The following table provides a matrix of the data and workloads that can be protected using Azure Backup. The Azure Backup solution column has links to the deployment documentation for that solution. Each Azure Backup component can be deployed in a Classic (Service Manager-deployment) or Resource Manager-deployment model environment.

> **IMPORTANT**
> Before you work with Azure resources, get familiar with the deployment models: Resource Manager, and classic.

DATA OR WORKLOAD	SOURCE ENVIRONMENT	AZURE BACKUP SOLUTION
Files and folders	Windows Server	Azure Backup agent, System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent)
Files and folders	Windows computer	Azure Backup agent, System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent)
Hyper-V virtual machine (Windows)	Windows Server	System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent)
Hyper-V virtual machine (Linux)	Windows Server	System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent)

DATA OR WORKLOAD	SOURCE ENVIRONMENT	AZURE BACKUP SOLUTION
Microsoft SQL Server	Windows Server	System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent)
Microsoft SharePoint	Windows Server	System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent)
Microsoft Exchange	Windows Server	System Center DPM (+ the Azure Backup agent), Azure Backup Server (includes the Azure Backup agent)
Azure IaaS VMs (Windows)	running in Azure	Azure Backup (VM extension)
Azure IaaS VMs (Linux)	running in Azure	Azure Backup (VM extension)

Linux support

The following table shows the Azure Backup components that have support for Linux.

COMPONENT	LINUX (AZURE ENDORSED) SUPPORT
Azure Backup (MARS) agent	No (Only Windows based agent)
System Center DPM	File-consistent backup of Linux Guest VMs on Hyper-V and VMWare (not available for Azure VM) VM restore of Hyper-V and VMWare Linux Guest VMs
Azure Backup Server	File-consistent backup of Linux Guest VMs on Hyper-V and VMWare (not available for Azure VM) VM restore of Hyper-V and VMWare Linux Guest VMs
Azure IaaS VM Backup	Application-consistent backup using pre-script and post-script framework Granular file recovery Restore all VM disks VM restore

Using Premium Storage VMs with Azure Backup

Azure Backup protects Premium Storage VMs. Azure Premium Storage is solid-state drive (SSD)-based storage designed to support I/O-intensive workloads. Premium Storage is attractive for virtual machine (VM) workloads. For more information about Premium Storage, see the article, Premium Storage: High-Performance Storage for Azure Virtual Machine Workloads.

Back up Premium Storage VMs

While backing up Premium Storage VMs, the Backup service creates a temporary staging location, named "AzureBackup-", in the Premium Storage account. The staging location is equal to the size of the recovery point snapshot. Be sure there is free space in the storage account to accommodate the temporary staging location. For more information, see the article, premium storage limitations. Once the backup job finishes, the staging location is deleted. The price of storage used for the staging location is consistent with all Premium storage pricing.

> **NOTE**
> Do not modify or edit the staging location.

Restore Premium Storage VMs

Premium Storage VMs can be restored to either Premium Storage or to normal storage. Restoring a Premium Storage VM recovery point back to Premium Storage is the typical process of restoration. However, it can be cost effective to restore a Premium Storage VM recovery point to standard storage. This type of restoration can be used if you need a subset of files from the VM.

Using managed disk VMs with Azure Backup

Azure Backup protects managed disk VMs. Managed disks free you from managing storage accounts of virtual machines and greatly simplify VM provisioning.

Back up managed disk VMs

Backing up VMs on managed disks is no different than backing up Resource Manager VMs. In the Azure portal, you can configure the backup job directly from the Virtual Machine view or from the Recovery Services vault view. You can back up VMs on managed disks through RestorePoint collections built on top of managed disks. Azure Backup also supports backing up managed disk VMs encrypted using Azure Disk encryption(ADE).

Restore managed disk VMs

Azure Backup allows you to restore a complete VM with managed disks or restore managed disks to a Resource Manager storage account. Azure manages the managed disks during the restore process. You (the customer) manage the storage account created as part of the restore process. For restoring managed encrypted VMs, keys and secrets of the VM should already exist in the key vault prior to restore.

What are the features of each Backup component?

The following sections provide tables that summarize the availability or support of various features in each Azure Backup component. See the information following each table for additional support or details.

Storage

FEATURE	AZURE BACKUP AGENT	SYSTEM CENTER DPM	AZURE BACKUP SERVER	AZURE IAAS VM BACKUP
Azure Backup vault				
Disk storage				
Tape storage				

FEATURE	AZURE BACKUP AGENT	SYSTEM CENTER DPM	AZURE BACKUP SERVER	AZURE IAAS VM BACKUP
Compression (in Backup vault)	●	●	●	
Incremental backup	●	●	●	●
Disk deduplication		◐	◐	

Key ● = Supported ◐ = Partially Supported *<blank>* = Not Supported

The Backup vault is the preferred storage target across all components. System Center DPM and Azure Backup Server also provide the option to have a local disk copy. However, only System Center DPM provides the option to write data to a tape storage device.

Compression

Backups are compressed to reduce the required storage space. The only component that does not use compression is the VM extension. The VM extension copies all backup data from your storage account to the Backup vault in the same region. No compression is used when transferring the data. Transferring the data without compression slightly inflates the storage used. However, storing the data without compression allows for faster restoration, should you need that recovery point.

Disk Deduplication

You can take advantage of deduplication when you deploy System Center DPM or Azure Backup Server on a Hyper-V virtual machine. Windows Server performs data deduplication (at the host level) on virtual hard disks (VHDs) that are attached to the virtual machine as backup storage.

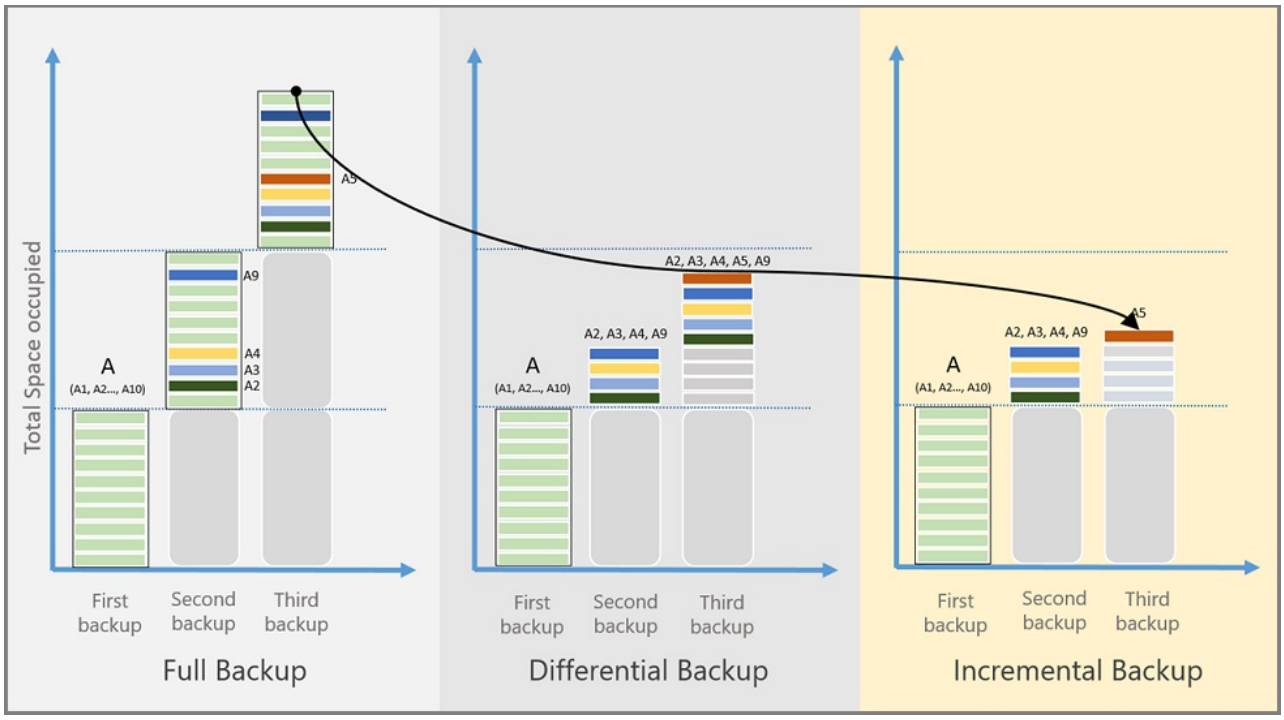
> **NOTE**
> Deduplication is not available in Azure for any Backup component. When System Center DPM and Backup Server are deployed in Azure, the storage disks attached to the VM cannot be deduplicated.

Incremental backup explained

Every Azure Backup component supports incremental backup regardless of the target storage (disk, tape, backup vault). Incremental backup ensures that backups are storage and time efficient, by transferring only those changes made since the last backup.

Comparing Full, Differential and Incremental backup

Storage consumption, recovery time objective (RTO), and network consumption varies for each type of backup method. To keep the backup total cost of ownership (TCO) down, you need to understand how to choose the best backup solution. The following image compares Full Backup, Differential Backup, and Incremental Backup. In the image, data source A is composed of 10 storage blocks A1-A10, which are backed up monthly. Blocks A2, A3, A4, and A9 change in the first month, and block A5 changes in the next month.



With **Full Backup**, each backup copy contains the entire data source. Full backup consumes a large amount of network bandwidth and storage, each time a backup copy is transferred.

Differential backup stores only the blocks that changed since the initial full backup, which results in a smaller amount of network and storage consumption. Differential backups don't retain redundant copies of unchanged data. However, because the data blocks that remain unchanged between subsequent backups are transferred and stored, differential backups are inefficient. In the second month, changed blocks A2, A3, A4, and A9 are backed up. In the third month, these same blocks are backed up again, along with changed block A5. The changed blocks continue to be backed up until the next full backup happens.

Incremental Backup achieves high storage and network efficiency by storing only the blocks of data that changed since the previous backup. With incremental backup, there is no need to take regular full backups. In the example, after the full backup is taken for the first month, changed blocks A2, A3, A4, and A9 are marked as changed and transferred for the second month. In the third month, only changed block A5 is marked and transferred. Moving less data saves storage and network resources, which decreases TCO.

Security

FEATURE	AZURE BACKUP AGENT	SYSTEM CENTER DPM	AZURE BACKUP SERVER	AZURE IAAS VM BACKUP
Network security (to Azure)	●	●	●	◐
Data security (in Azure)	●	●	●	◐

Key ● = Supported ◐ = Partially Supported *<blank>* = Not Supported

Network security

All backup traffic from your servers to the Backup vault is encrypted using Advanced Encryption Standard 256. The backup data is sent over a secure HTTPS link. The backup data is also stored in the Backup vault in encrypted form. Only you, the Azure customer, have the passphrase to unlock this data. Microsoft cannot decrypt the backup data at any point.

> **WARNING**
> Once you establish the Backup vault, only you have access to the encryption key. Microsoft never maintains a copy of your encryption key, and does not have access to the key. If the key is misplaced, Microsoft cannot recover the backup data.

Data security

Backing up Azure VMs requires setting up encryption *within* the virtual machine. Use BitLocker on Windows virtual machines and **dm-crypt** on Linux virtual machines. Azure Backup does not automatically encrypt backup data that comes through this path.

Network

FEATURE	AZURE BACKUP AGENT	SYSTEM CENTER DPM	AZURE BACKUP SERVER	AZURE IAAS VM BACKUP
Network compression (to **backup server**)		●	●	
Network compression (to **backup vault**)	●	●	●	
Network protocol (to **backup server**)		TCP	TCP	
Network protocol (to **backup vault**)	HTTPS	HTTPS	HTTPS	HTTPS

Key ● = Supported *<blank>* = Not Supported

The VM extension (on the IaaS VM) reads the data directly from the Azure storage account over the storage network, so it is not necessary to compress this traffic.

If you are backing up data to a System Center DPM or Azure Backup Server, compress data going from the primary server to the backup server. Compressing data before backing it up to DPM or Azure Backup Server, saves bandwidth.

Network Throttling

The Azure Backup agent offers network throttling, which allows you to control how network bandwidth is used during data transfer. Throttling can be helpful if you need to back up data during work hours but do not want the backup process to interfere with other internet traffic. Throttling for data transfer applies to back up and restore activities.

Backup and retention

Azure Backup has a limit of 9999 recovery points, also known as backup copies or snapshots, per *protected instance*. A protected instance is a computer, server (physical or virtual), or workload configured to back up data to Azure. For more information, see the section, What is a protected instance. An instance is protected once a backup copy of data has been saved. The backup copy of data is the protection. If the source data was lost or became corrupt, the backup copy could restore the source data. The following table shows the maximum backup frequency for each component. Your backup policy configuration determines how quickly you consume the recovery points. For example, if you create a recovery point each day, then you can retain recovery points for 27 years before you run out. If you take a monthly recovery point, you can retain recovery points for 833 years before you run out. The Backup service does not set an expiration time limit on a recovery point.

	AZURE BACKUP AGENT	SYSTEM CENTER DPM	AZURE BACKUP SERVER	AZURE IAAS VM BACKUP
Backup frequency (to Backup vault)	Three backups per day	Two backups per day	Two backups per day	One backup per day
Backup frequency (to disk)	Not applicable	• Every 15 minutes for SQL Server • Every hour for other workloads	• Every 15 minutes for SQL Server • Every hour for other workloads	Not applicable
Retention options	Daily, weekly, monthly, yearly	Daily, weekly, monthly, yearly	Daily, weekly, monthly, yearly	Daily, weekly, monthly, yearly
Maximum recovery points per protected instance	9999	9999	9999	9999
Maximum retention period	Depends on backup frequency	Depends on backup frequency	Depends on backup frequency	Depends on backup frequency
Recovery points on local disk	Not applicable	• 64 for File Servers, • 448 for Application Servers	• 64 for File Servers, • 448 for Application Servers	Not applicable
Recovery points on tape	Not applicable	Unlimited	Not applicable	Not applicable

What is a protected instance

A protected instance is a generic reference to a Windows computer, a server (physical or virtual), or SQL database that has been configured to back up to Azure. An instance is protected once you configure a backup policy for the computer, server, or database, and create a backup copy of the data. Subsequent copies of the backup data for that protected instance (which are called recovery points), increase the amount of storage consumed. You can create up to 9999 recovery points for a protected instance. If you delete a recovery point from storage, it does not count against the 9999 recovery point total. Some common examples of protected instances are virtual machines, application servers, databases, and personal computers running the Windows operating system. For example:

- A virtual machine running the Hyper-V or Azure IaaS hypervisor fabric. The guest operating systems for the virtual machine can be Windows Server or Linux.
- An application server: The application server can be a physical or virtual machine running Windows Server and workloads with data that needs to be backed up. Common workloads are Microsoft SQL Server, Microsoft Exchange server, Microsoft SharePoint server, and the File Server role on Windows Server. To back up these workloads you need System Center Data Protection Manager (DPM) or Azure Backup Server.
- A personal computer, workstation, or laptop running the Windows operating system.

What is the vault credential file?

The vault credentials file is a certificate generated by the portal for each Backup vault. The portal then uploads the public key to the Access Control Service (ACS). The private key is provided to you when downloading the credentials. Use it to register the computers you protect. The private key is what allows you to authenticate the servers or computers to send backup data to a particular Backup vault.

You only use the vault credential to register the servers or computers. However, take care with the vault credentials, if it is lost or obtained by others, the vault credentials can be used to register other machines against the same

vault. Since the backup data is encrypted using a passphrase, that only you can access, existing backup data cannot be compromised. Vault credentials expire after 48 hours. While you can download the Backup vault's vault credentials as often as you like, only the latest credentials can be used for registration.

How does Azure Backup differ from Azure Site Recovery?

Azure Backup and Azure Site Recovery are related in that both services back up data and can restore that data. However, these services have different value propositions.

Azure Backup protects data on-premises and in the cloud. Azure Site Recovery coordinates virtual-machine and physical-server replication, failover, and failback. Both services are important because your disaster recovery solution needs to keep your data safe and recoverable (Backup) *and* keep your workloads available (Site Recovery) when outages occur.

The following concepts can help you make important decisions around backup and disaster recovery.

CONCEPT	DETAILS	BACKUP	DISASTER RECOVERY (DR)
Recovery point objective (RPO)	The amount of acceptable data loss if a recovery needs to be done.	Backup solutions have wide variability in their acceptable RPO. Virtual machine backups usually have an RPO of one day, while database backups have RPOs as low as 15 minutes.	Disaster recovery solutions have low RPOs. The DR copy can be behind by a few seconds or a few minutes.
Recovery time objective (RTO)	The amount of time that it takes to complete a recovery or restore.	Because of the larger RPO, the amount of data that a backup solution needs to process is typically much higher, which leads to longer RTOs. For example, it can take days to restore data from tapes, depending on the time it takes to transport the tape from an off-site location.	Disaster recovery solutions have smaller RTOs because they are more in sync with the source. Fewer changes need to be processed.
Retention	How long data needs to be stored	For scenarios that require operational recovery (data corruption, inadvertent file deletion, OS failure), backup data is typically retained for 30 days or less. From a compliance standpoint, data might need to be stored for months or even years. Backup data is ideally suited for archiving in such cases.	Disaster recovery needs only operational recovery data, which typically takes a few hours or up to a day. Because of the fine-grained data capture used in DR solutions, using DR data for long-term retention is not recommended.

Next steps

Use one of the following tutorials for detailed, step-by-step, instructions for protecting data on Windows Server, or protecting a virtual machine (VM) in Azure:

- Back up Files and Folders
- Backup Azure Virtual Machines

For details about protecting other workloads, try one of these articles:

- Back up your Windows Server
- Back up application workloads
- Backup Azure IaaS VMs

What is Site Recovery?

3/14/2017 • 3 min to read • Edit Online

Welcome to the Azure Site Recovery service! This article provides a quick overview of the service.

Outages are causes by natural events and operational failures. Your organization needs a business continuity and disaster recovery (BCDR) strategy so that, during planned and unplanned downtime, data stays safe, apps remain available, and business recovers to normal working conditions as soon as possible.

Azure Recovery Services contribute to your BCDR strategy. The Azure Backup service keeps your data safe and recoverable. Site Recovery replicates, fails over, and recovers workloads, so that they remain available when failure occurs.

What does Site Recovery provide?

- **Disaster recovery in the cloud**—You can replicate workloads running on VMs and physical servers to Azure, rather than to a secondary site. This eliminates the cost and complexity of maintaining a secondary datacenter.
- **Flexible replication for hybrid environments**—You can replicate any workload running on supported on-premises Hyper-V VMs, VMware VMs, and Windows/Linux physical servers.
- **Migration**—You can use Site Recovery to migrate on-premises AWS instances to Azure VMs, or to migrate Azure VMs between Azure regions.
- **Simplified BCDR**—You can deploy replication from a single location in the Azure portal. You can run simple failovers and failback of single and multiple machines.
- **Resilience**—Site recovery orchestrates replication and failover, without intercepting application data. Replicated data is stored in Azure storage, with the resilience that provides. When failover occurs, Azure VMs are created based on the replicated data.
- **Replication performance**—Site Recovery provides replication frequency as low as 30 seconds for Hyper-V, and continuous replication for VMware. You can set recovery point objective (RPO) thresholds to control how often data recovery points are created, and you can reduce recovery time objective (RTO) with Site Recovery's automated recovery process, and integration with Azure Traffic Manager
- **Application consistency**—Machines replicate using application-consistent snapshots. In addition to capturing disk data, application-consistent snapshots capture all data in memory, and all transactions in process.
- **Testing without disruption**—You can easily run test failovers to support disaster recovery drills, without affecting production environments.
- **Flexible failover and recovery**—You can run planned failovers for expected outages with zero-data loss, or unplanned failovers with minimal data loss (depending on replication frequency) for unexpected disasters. You can easily fail back to your primary site when it's available again.
- **Custom recovery plans**—Recovery plans allow you to model and customize failover and recovery of multi-tier applications that are spread over multiple VMs. You order groups within plans, and add scripts and manual actions. Recovery plans can be integrated with Azure automation runbooks.
- **Multi-tier apps**—You can create recovery plans for sequenced failover and recovery of multi-tiered apps. You can group machines in different tiers (for example database, web, app) within a recovery plan, and customize how each group fails over and starts up.
- **Integration with existing BCDR technologies**—Site Recovery integrates with other BCDR technologies. For example, you can use Site Recovery to protect the SQL Server backend of corporate workloads, including native support for SQL Server AlwaysOn, to manage the failover of availability groups.
- **Integration with the automation library**—A rich Azure Automation library provides production-ready, application-specific scripts that can be downloaded and integrated with Site Recovery.

- **Simple network management**—Advanced network management in Site Recovery and Azure simplifies application network requirements, including reserving IP addresses, configuring load-balancers, and integrating Azure Traffic Manager for efficient network switchovers.

What's supported?

SUPPORTED	DETAILS
Which regions are supported for Site Recovery?	Supported regions
What can I replicate?	On-premises VMware VMs, Hyper-V VMs, Windows and Linux physical servers.
What operating systems do replicated machines need?	Supported operating systems for VMware VMs For Hyper-V VMs, any guest OS supported by Azure and Hyper-V is supported. Operating systems for physical servers
Where can I replicate to?	To Azure storage, or to a secondary datacenter For Hyper-V, only VMs on Hyper-V hosts managed in System Center VMM clouds can replicate to a secondary datacenter.
What VMware servers/hosts do I need?	VMware VMs you want to replicate can be managed by supported vSphere hosts/vCenter servers
What workloads can I replicate	You can replicate any workload running on a supported replication machine. In addition, the Site Recovery team have performed app-specific testing for a number of apps.

Which Azure portal?

- Site Recovery can be deployed in both the newer Azure portal, and in the Azure classic portal .
- In the Azure classic portal, you can support Site Recovery with the classic services management model.
- In the Azure portal, you can support the classic model, or the newer Resource Manager deployment model.
- The classic portal should only be used to maintain existing Site Recovery deployments. You can't create new vaults in the classic portal.

Next steps

- Read more about workload support
- Learn more about Site Recovery architecture and components

Monitoring resources in Operations Management Suite Security and Audit Solution

3/30/2017 • 5 min to read • Edit Online

This document helps you use OMS Security and Audit capabilities to monitor your resources and identify security issues.

What is OMS?

Microsoft Operations Management Suite (OMS) is Microsoft's cloud based IT management solution that helps you manage and protect your on-premises and cloud infrastructure. For more information about OMS, read the article Operations Management Suite.

Monitoring resources

Whenever is possible, you will want to prevent security incidents from happening in the first place. However, it is impossible to prevent all security incidents. When a security incident does happen, you will need to ensure that its impact is minimized. There are three critical recommendations that can be used to minimize the number and the impact of security incidents:

- Routinely assess vulnerabilities in your environment.
- Routinely check all computer systems and network devices to ensure that they have all of the latest patches installed.
- Routinely check all logs and logging mechanisms, including operating system event logs, application specific logs and intrusion detection system logs.

OMS Security and Audit solution enables IT to actively monitor all resources, which can help minimize the impact of security incidents. OMS Security and Audit has security domains that can be used for monitoring resources. The security domains provides quick access to a options, for security monitoring the following domains will be covered in more details:

- Malware assessment
- Update assessment
- Identity and Access

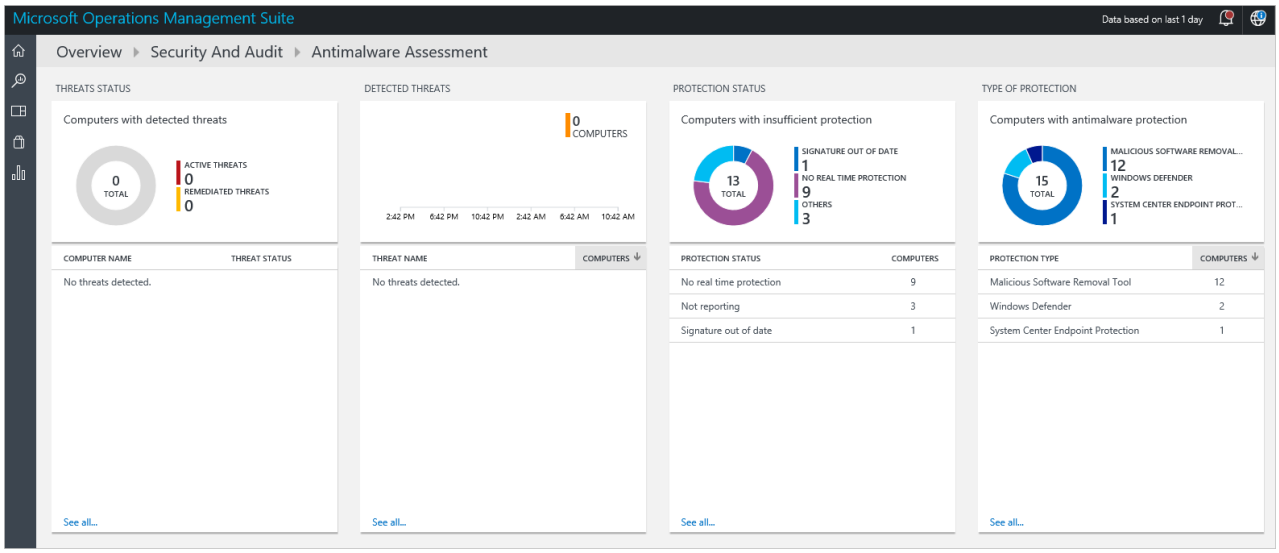
> **NOTE**
> for an overview of all these options, read Getting started with Operations Management Suite Security and Audit Solution.

Monitoring system protection

In a defense in depth approach, every layer of protection is important for the overall security state of your asset. Computers with detected threats and computers with insufficient protection are shown in the Malware Assessment tile under Security Domains. By using the information on the Malware Assessment, you can identify a plan to apply protection to the servers that need it. To access this option follow the steps below:

1. In the **Microsoft Operations Management Suite** main dashboard click **Security and Audit** tile.

2. In the **Security and Audit** dashboard, click **Antimalware Assessment** under **Security Domains**. The **Antimalware Assessment** dashboard appears as shown below:

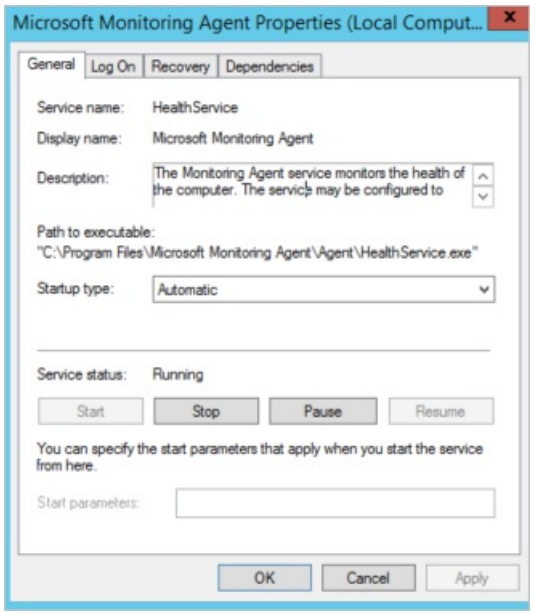


You can use the **Malware Assessment** dashboard to identify the following security issues:

- **Active threats**: computers that were compromised and have active threats in the system.
- **Remediated threats**: computers that were compromised but the threats were remediated.
- **Signature out of date**: computers that have malware protection enabled but the signature is out of date.
- **No real time protection**: computers that don't have antimalware installed.

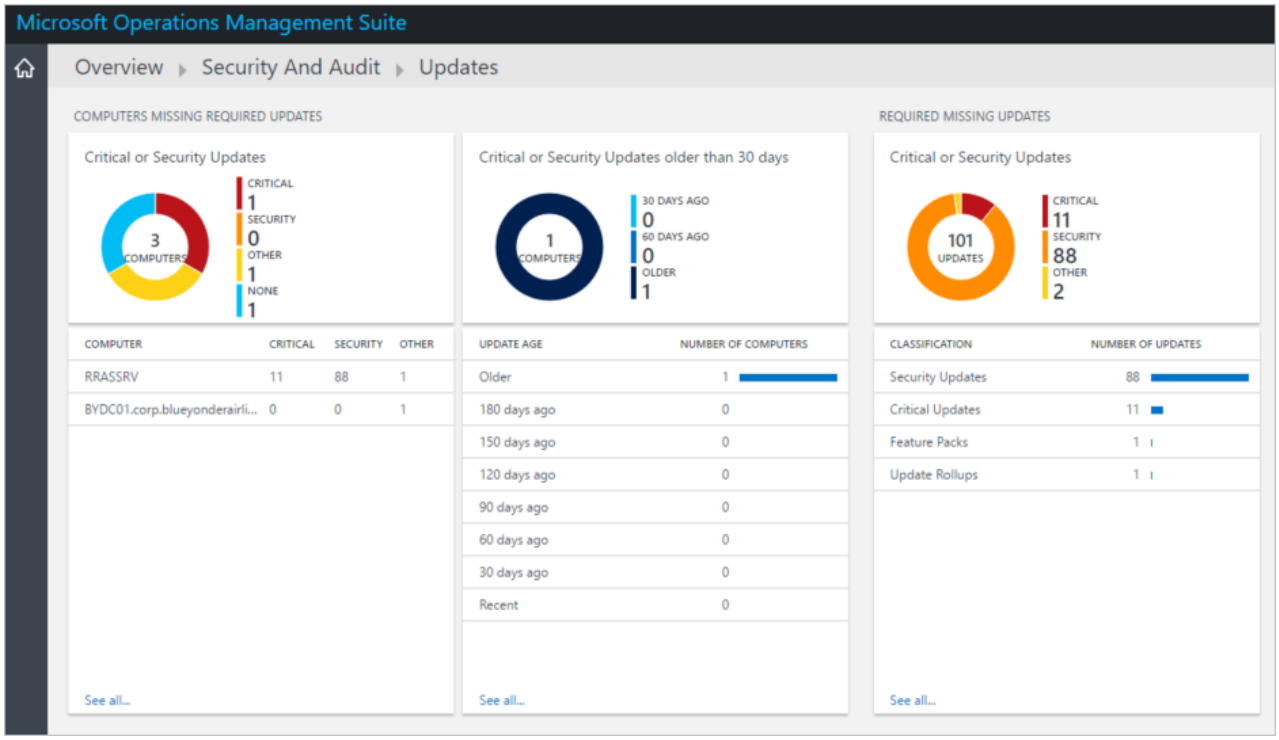
Monitoring updates

Applying the most recent security updates is a security best practice and it should be incorporated in your update management strategy. Microsoft Monitoring Agent service (HealthService.exe) reads update information from monitored computers and then sends this updated information to the OMS service in the cloud for processing. The Microsoft Monitoring Agent service is configured as an automatic service and it should be always running in the target computer.

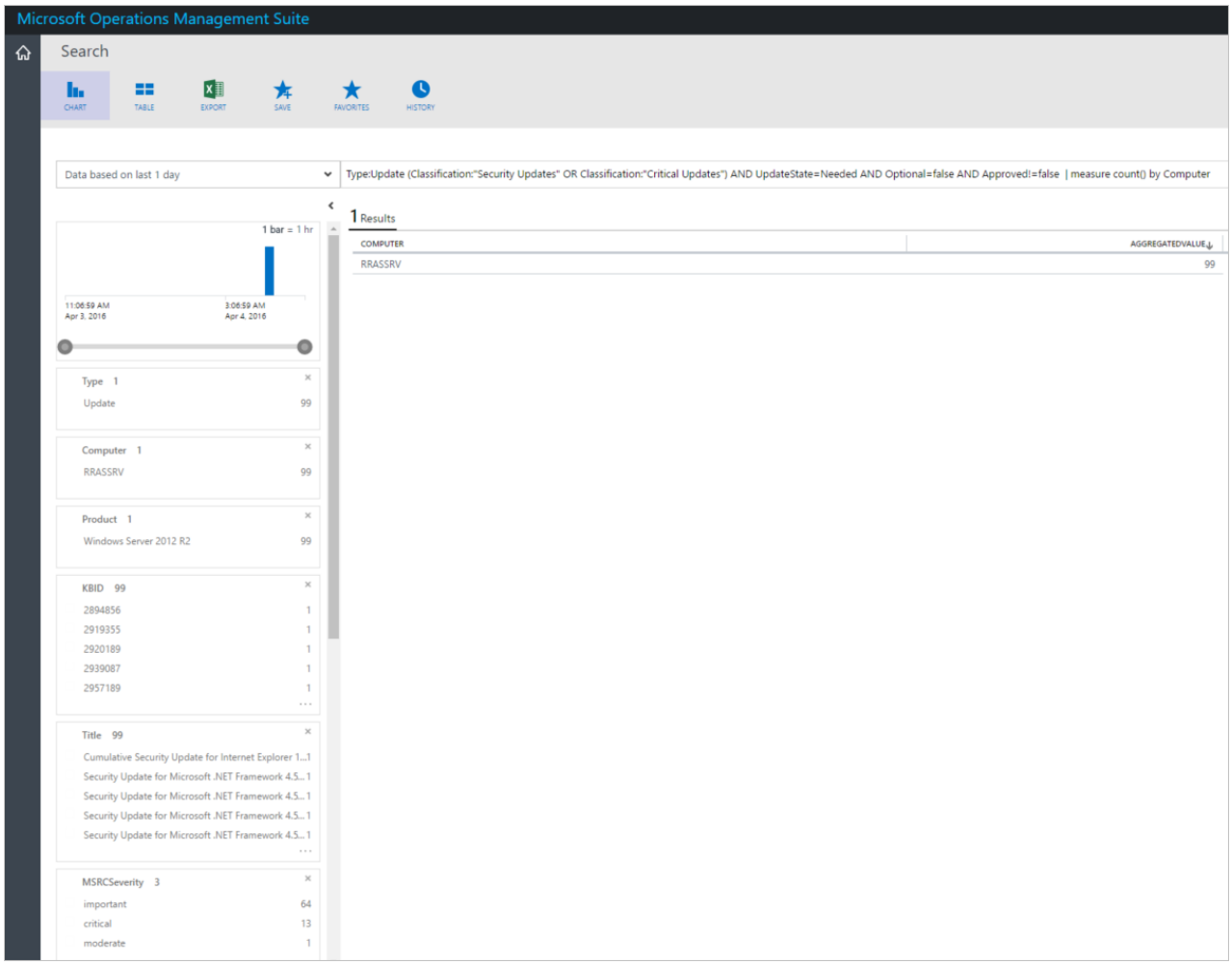


Logic is applied to the update data and the cloud service records the data. If missing updates are found, they are shown on the **Updates** dashboard. You can use the **Updates** dashboard to work with missing updates and develop a plan to apply them to the servers that need them. Follow the steps below to access the **Updates** dashboard:

1. In the **Microsoft Operations Management Suite** main dashboard click **Security and Audit** tile.
2. In the **Security and Audit** dashboard, click **Update Assessment** under **Security Domains**. The Update dashboard appears as shown below:



In this dashboard you can perform an update assessment to understand the current state of your computers and address the most critical threats. By using the **Critical or Security Updates** tile, IT administrators will be able to access detailed information about the updates that are missing as shown below:



This report include critical information that can be used to identify the type of threat this system is vulnerable to, which includes the Microsoft KB articles associated with the security update and the MS Bulletin that has more details about the vulnerability.

Monitoring identity and access

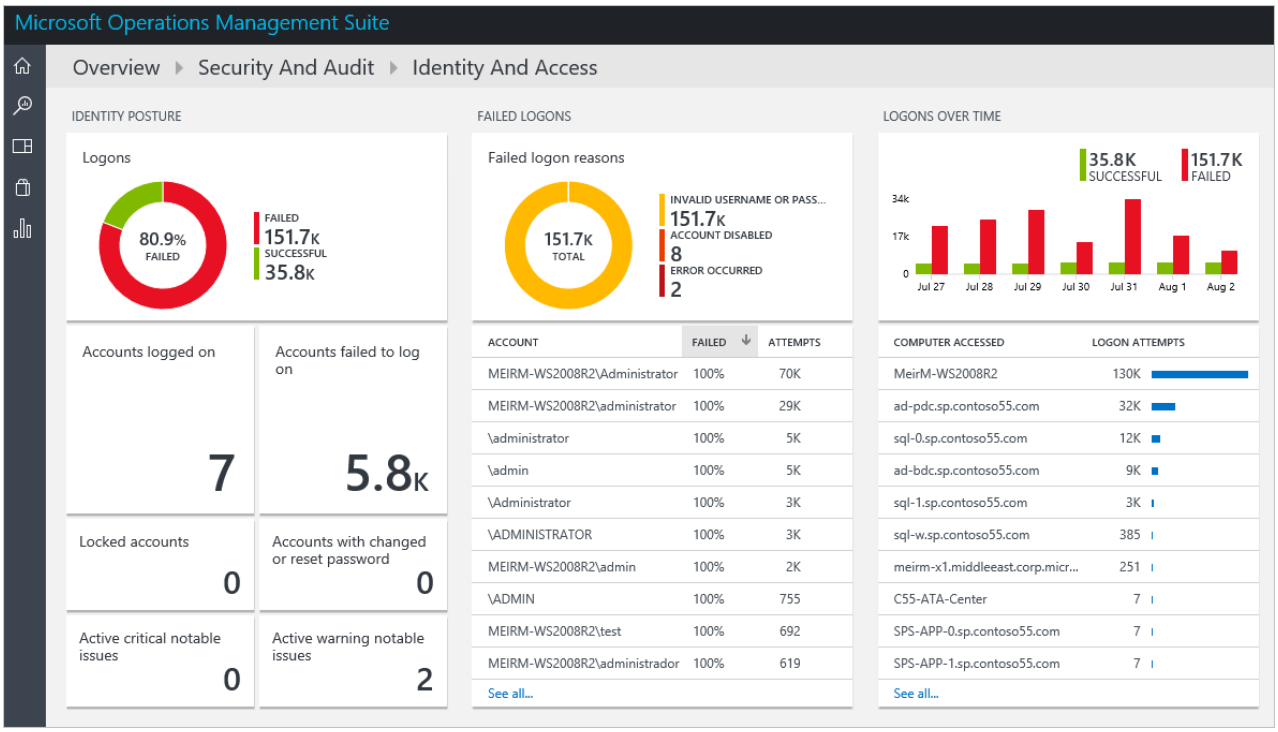
With users working from anywhere, using different devices and accessing a vast amount of cloud and on-premises apps, it is imperative that their credentials are protected. Credential theft attacks are those in which an attacker initially gains access to a regular user's credentials to access a system within the network. Many times, this initial attack is only a way to get access to the network, the ultimate goal is to discover privilege accounts.

Attackers will stay in the network, using freely available tooling to extract credentials from the sessions of other logged-on accounts. Depending on the system configuration, these credentials can be extracted in the form of hashes, tickets, or even plaintext passwords.

> **NOTE**
> machines that are directly exposed to the Internet will see many failed attempts that try to login using all kind of well-known usernames (e.g. Administrator). In most cases it is OK if the well-known usernames are not used and if the password is strong enough.

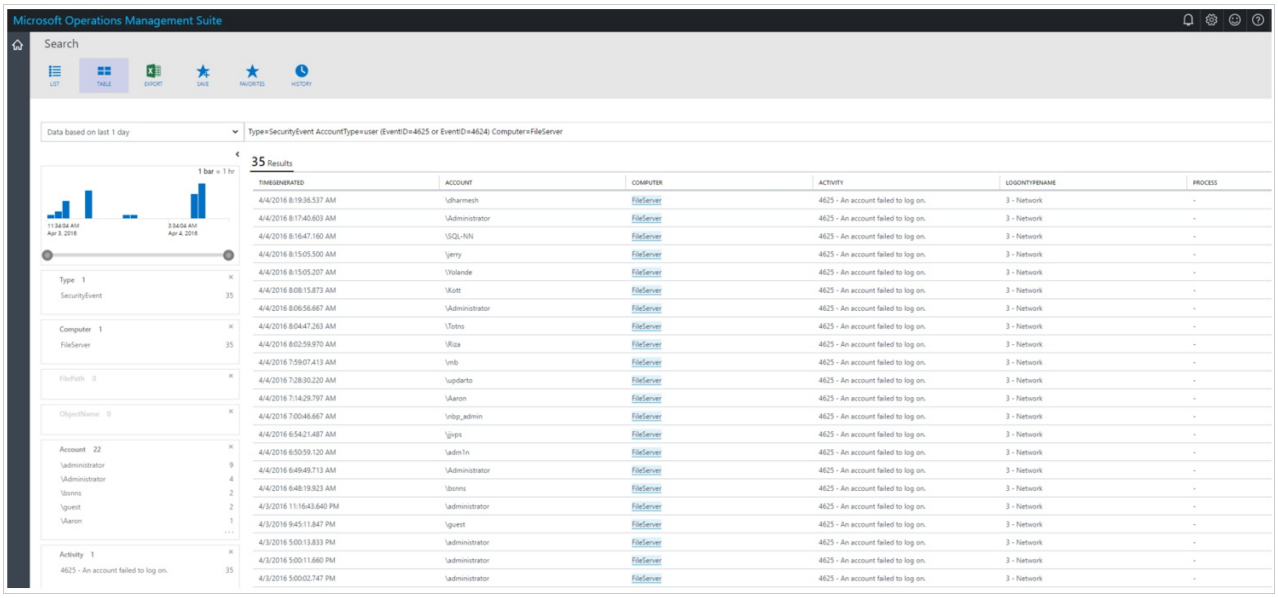
It is possible to identify these intruders before they compromise a privilege account. You can leverage **OMS Security and Audit Solution** to monitor identity and access. Follow the steps below to access the **Identity and Access** dashboard:

1. In the **Microsoft Operations Management Suite** main dashboard click Security and Audit tile.
2. In the **Security and Audit** dashboard, click **Identity and Access** under **Security Domains**. The **Identity and Access** dashboard appears as shown below:



As part of your regular monitoring strategy, you must include identity monitoring. IT Admin should look if there is a specific valid username that has many attempts. This might indicate either attacker that acquired the real username and try to brute force or an automatic tool that uses hard-coded password that expired.

This dashboard enable IT to quickly identify potential threats related to identity and access to company's resources. It is particular important to also identify potential trends, for example in the Logons Over Time tile, you can see over period of time how many times a failed logon attempt was performed. In this case the computer **FileServer** received 35 logon attempts. You can explore more details about this computer by clicking on it.



The report generated for this computer brings valuable details about this pattern. Noticed that the **ACCOUNT** column gives you the user account that was used to try to access the system, the **TIMEGENERATED** column gives you the time interval in which the attempt was done and the **LOGONTYPENAME** column gives you the location where this attempt was done. If these attempts were performed locally in the system by a program, the **PROCESS** column would be showing the process's name. In scenarios where the logon attempt is coming from a program, you already have the process name available and now you can perform further investigation in the target system.

See also

In this document, you learned how to use OMS Security and Audit solution to monitor your resources. To learn

more about OMS Security, see the following articles:

- Operations Management Suite (OMS) overview
- Getting started with Operations Management Suite Security and Audit Solution
- Monitoring and Responding to Security Alerts in Operations Management Suite Security and Audit Solution

Monitoring and responding to security alerts in Operations Management Suite Security and Audit Solution

3/30/2017 • 3 min to read • Edit Online

This document helps you use the threat intelligence option available in OMS Security and Audit to monitor and respond to security alerts.

What is OMS?

Microsoft Operations Management Suite (OMS) is Microsoft's cloud based IT management solution that helps you manage and protect your on-premises and cloud infrastructure. For more information about OMS, read the article Operations Management Suite.

Threat intelligence

In an enterprise environment where users have broad access to the network and use a variety of devices to connect to corporate data, it is imperative that you can actively monitor your resources and quickly respond to security incidents. This is particular important from the security lifecycle perspective because some cybersecurity threats may not raise alerts or suspicious activities that can be identified by traditional security technical controls.

By using the **Threat Intelligence** option available in OMS Security and Audit, IT administrators can identify security threats against the environment, for example, identify if a particular computer is part of a botnet. Computers can become nodes in a botnet when attackers illicitly install malware that secretly connects this computer to the command and control. It can also identify potential threats coming from underground communication channels, such as darknet.

In order to build this threat intelligence, OMS Security and Audit use data coming from multiple sources within Microsoft. OMS Security and Audit will leverage this data to identify potential threats against your environment.

The Threat Intelligence pane is composed by three major options:

- Servers with outbound malicious traffic
- Detected threats types
- Threat intelligence map

> **NOTE**
> for an overview of all these options, read Getting started with Operations Management Suite Security and Audit Solution.

Responding to security alerts

One of the steps of a security incident response process is to identify the severity of the compromise system(s). In this phase you should perform the following tasks:

- Determine the nature of the attack
- Determine the attack point of origin
- Determine the intent of the attack. Was the attack specifically directed at your organization to acquire specific information, or was it random?

- Identify the systems that have been compromised
- Identify the files that have been accessed and determine the sensitivity of those files

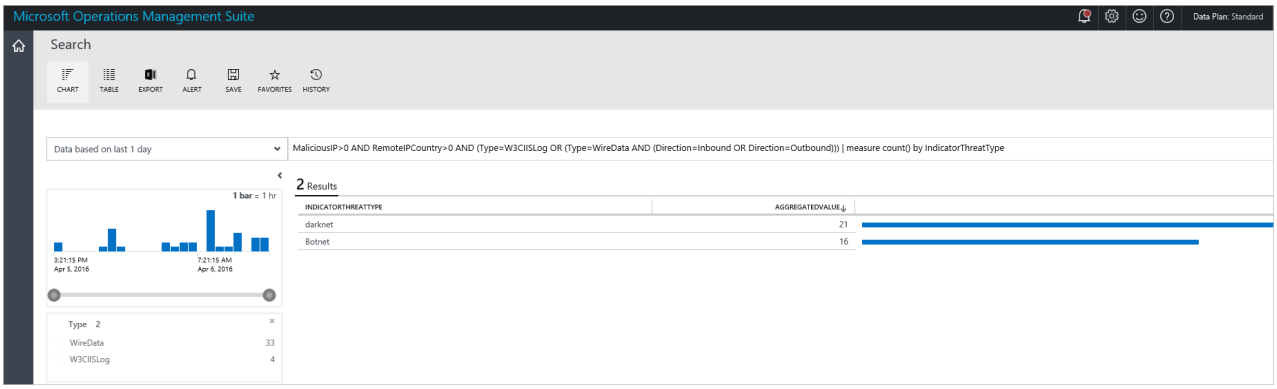
You can leverage **Threat Intelligence** information in OMS Security and Audit solution to help with these tasks. Follow the steps below to access this **Threat Intelligence** options:

1. In the **Microsoft Operations Management Suite** main dashboard click **Security and Audit** tile.

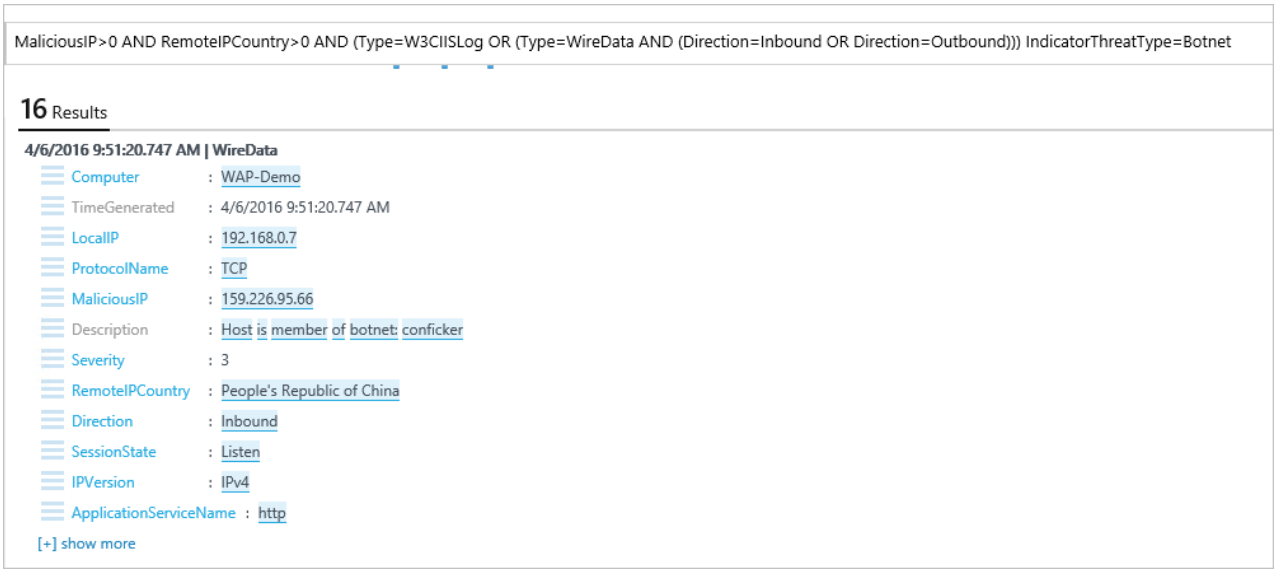
2. In the **Security and Audit** dashboard, you will see the **Threat Intelligence** options in the right, as shown below:

These three tiles will give you an overview of the current threats. In the **Server with outbound malicious traffic** you will be able to identify if there is any computer that you are monitoring (inside or outside of your network) that is sending malicious traffic to the Internet.

The **Detected threat types** tile shows a summary of the threats that are current "in the wild", if you click on this tile you will see more details about these threats as show below:

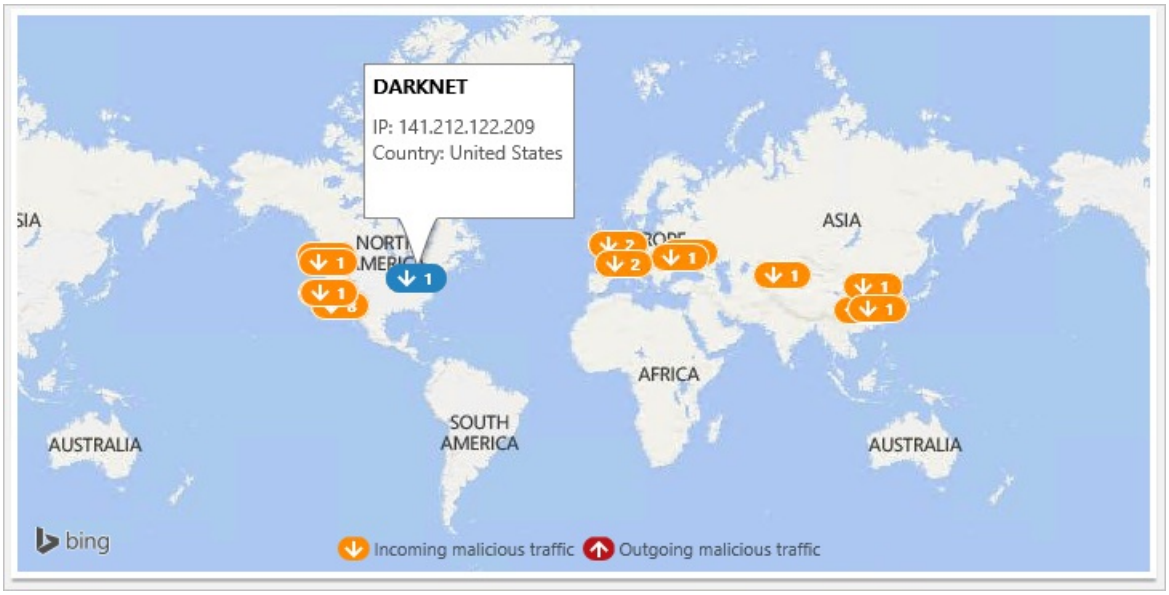


You can extract more information about each threat by clicking on it. The example below shows more details about Botnet:



As described in the beginning of this section, this information can be very useful during an incident response case. It can also be important during a forensic investigation, where you need to find the source of the attack, which system was compromised and the timeline. In this report you can easily identify some key details about the attack, such as: the source of the attack, the local IP that was compromised and the current session state of the connection.

The **threat intelligence map** will help you to identify the current locations around the globe that have malicious traffic. There are orange (incoming) and red (outgoing) arrows in this map that identify the traffic direction, if you click in one of these arrows, it will show the type of threat and the traffic direction as shown below:



NOTE

You can see a demonstration on how to use this capability during an incident response process by watching the presentation Mitigate datacenter security threats with guided investigation using Operations Management Suite delivered at Microsoft Ignite.

See also

In this document, you learned how to use the **Threat Intelligence** option in OMS Security and Audit solution to respond to security alerts. To learn more about OMS Security, see the following articles:

- Operations Management Suite (OMS) overview
- Getting started with Operations Management Suite Security and Audit Solution
- Monitoring Resources in Operations Management Suite Security and Audit Solution

Baseline Assessment in Operations Management Suite Security and Audit Solution

3/30/2017 • 3 min to read • Edit Online

This document helps you to use Operations Management Suite (OMS) Security and Audit Solution baseline assessment capabilities to access the secure state of your monitored resources.

What is Baseline Assessment?

Microsoft, together with industry and government organizations worldwide, defines a Windows configuration that represents highly secure server deployments. This configuration is a set of registry keys, audit policy settings, and security policy settings along with Microsoft's recommended values for these settings. This set of rules is known as Security baseline. OMS Security and Audit baseline assessment capability can seamlessly scan all your computers for compliance.

There are three types of rules:

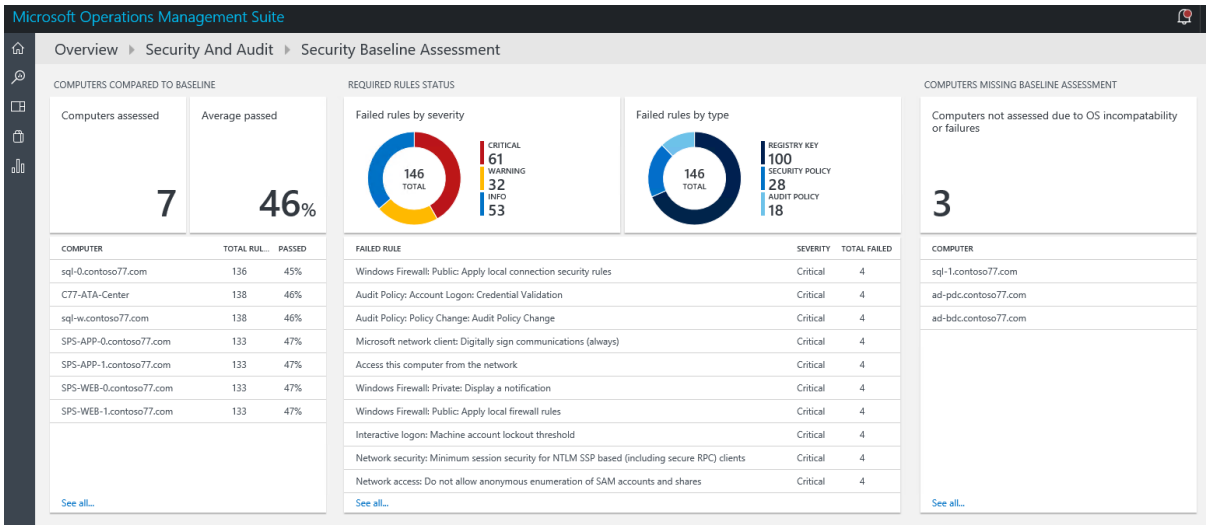
- **Registry rules**: check that registry keys are set correctly.
- **Audit policy rules**: rules regarding your audit policy.
- **Security policy rules**: rules regarding the user's permissions on the machine.

> **NOTE**
>
> Read Use OMS Security to assess the Security Configuration Baseline for a brief overview of this feature.

Security Baseline Assessment

You can review your current security baseline assessment for all computers that are monitored by OMS Security and Audit using the dashboard. Execute the following steps to access the security baseline assessment dashboard:

1. In the **Microsoft Operations Management Suite** main dashboard, click **Security and Audit** tile.
2. In the **Security and Audit** dashboard, click **Baseline Assessment** under **Security Domains**. The **Security Baseline Assessment** dashboard appears as shown in the following image:

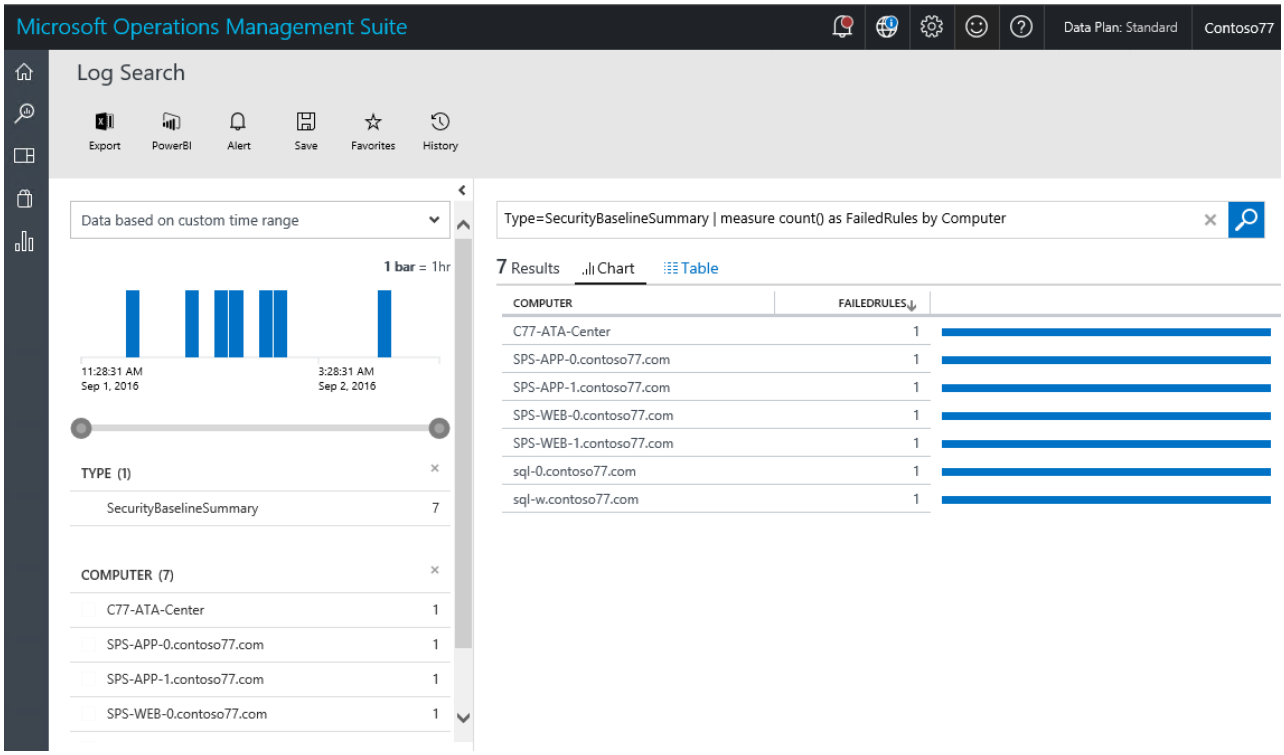


This dashboard is divided in three major areas:

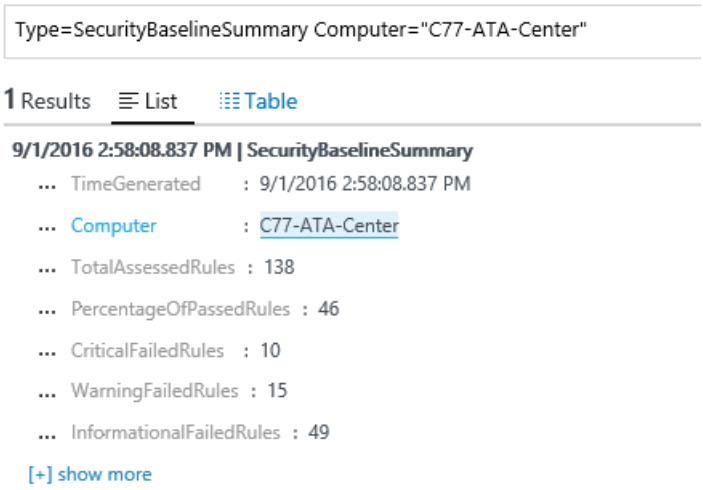
- **Computers compared to baseline**: this section gives a summary of the number of computers that were accessed and the percentage of computers that passed the assessment. It also gives the top 10 computers and the percentage result for the assessment.
- **Required Rules Status**: this section has the intent to bring awareness of the failed rules by severity and failed rules by type. By looking to the first graph you can quickly identify if most the failed rules are critical, or not. It also gives a list of the top 10 failed rules and their severity. The second graph shows the type of rule that failed during the assessment.
- **Computers missing baseline assessment**: this section list the computers that were not accessed due to operating system incompatibility or failures.

Accessing computers compared to baseline

Ideally all your computers are be compliant with the security baseline assessment. However it is expected that in some circumstances this doesn't happen. As part of the security management process, it is important to include reviewing the computers that failed to pass all security assessment tests. A quick way to visualize that is by selecting the option **Computers accessed** located in the **Computers compared to baseline** section. You should see the log search result showing the list of computers as shows in the following screen:



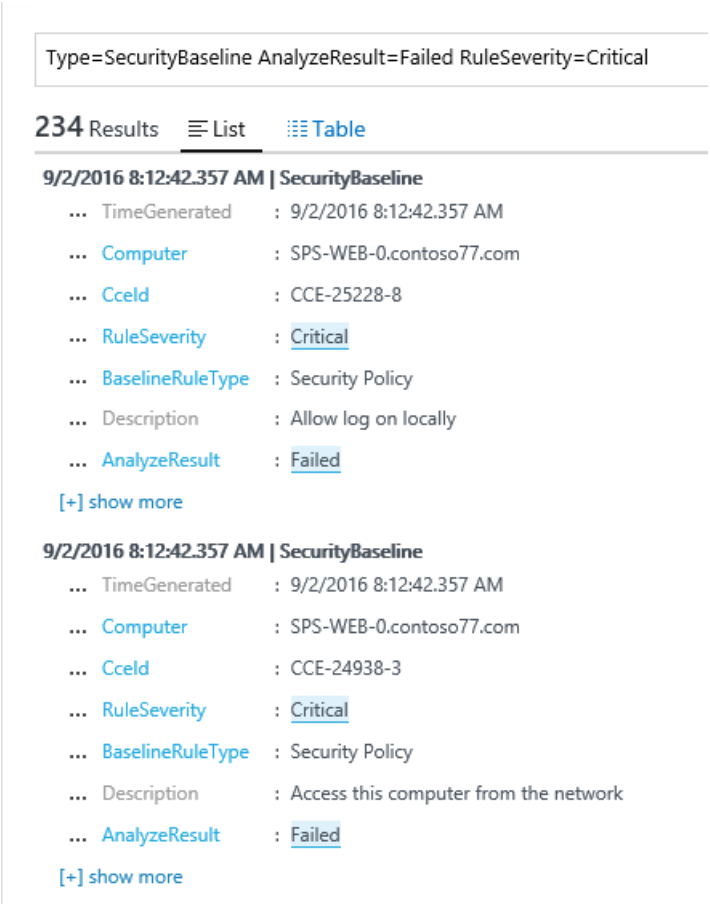
The search result is shown in a table format, where the first column has the computer name and the second color has the number of rules that failed. To retrieve the information regarding the type of rule that failed, click in the number of failed rules besides the computer name. You should see a result similar to the one shown in the following image:



In this search result, you have the total of accessed rules, the number of critical rules that failed, the warning rules and the information failed rules.

Accessing required rules status

After obtaining the information regarding the percentage number of computers that passed the assessment, you may want to obtain more information about which rules are failing according to the criticality. This visualization helps you to prioritize which computers should be addressed first to ensure they will be compliant in the next assessment. Hover over the Critical part of the graph located in the **Failed rules by severity** tile, under **Required rules status** and click it. You should see a result similar to the following screen:



In this log result you see the type of baseline rule that failed, the description of this rule, and the Common Configuration Enumeration (CCE) ID of this security rule. These attributes should be enough to perform a corrective action to fix this problem in the target computer.

> **NOTE**
>
> For more information about CCE, access the National Vulnerability Database.

Accessing computers missing baseline assessment

OMS supports the domain member and Domain Controller baseline profile on Windows Server 2008 R2 up to Windows Server 2012 R2. Windows Server 2016 baseline isn't final yet and will be added as soon as it is published. All other operating systems scanned via OMS Security and Audit baseline assessment appears under the **Computers missing baseline assessment** section.

See also

In this document, you learned about OMS Security and Audit baseline assessment. To learn more about OMS Security, see the following articles:

- Operations Management Suite (OMS) overview
- Monitoring and Responding to Security Alerts in Operations Management Suite Security and Audit Solution
- Monitoring Resources in Operations Management Suite Security and Audit Solution

Identify malware using the Malware Assessment solution in Log Analytics

3/27/2017 • 3 min to read • Edit Online

You can use the Antimalware solution in Log Analytics to report on the status of antimalware protection in your infrastructure. Installing the solution updates the OMS agent and base configuration for OMS. Antimalware protection status and detected threats on the monitored servers are read, and then the data is sent to the Log Analytics service in the cloud for processing. Logic is applied to the received data and the cloud service records the data. Servers with detected threats and servers with insufficient protection are shown in the **Antimalware** dashboard. By using the information on the **Antimalware** dashboard, you can identify a plan to apply protection to the servers that need it.

Installing and configuring the solution

Use the following information to install and configure the solution.

- In order to use the Malware Assessment solution, you must subscribe to the Security & Compliance solution offering.
- Add the Malware Assessment solution to your OMS workspace from Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery. There is no further configuration required.

Use Antimalware

Log Analytics reports antimalware status for:

- Computers running Windows Defender on Windows 8, Windows 8.1, Windows 10, and Windows Server 2016 TP4 or later
- Windows Security Center (WSC) on Windows 8, Windows 8.1, Windows 10, Windows Server 2016 TP4 or later
- Servers running System Center Endpoint Protection (v4.5.216 or later), Azure virtual machines with the antimalware extension, and Windows Malicious Software Removal Tool (MSRT)
- Servers with Windows Management Framework 3 (or later) WMF 3.0, WMF 4.0.
- Symantec Endpoint Protection 12.x and 14.x versions
- Trend Micro Deep Security version 9.6

In addition to detecting when 3rd party solutions are installed, an additional assessment is also done to determine whether protection by agents is operational. Specifically, OMS Security tests to see if the antimalware agents from these vendors on the monitored servers are:

- Enabled
- Running scans at regular intervals
- Using signatures no older than seven days

The antimalware solution does not currently report on:

- Servers running Windows Server 2008 and earlier
- Web and Worker roles in Microsoft Azure

You can help us prioritize the addition of new features by voting or adding a new suggestion on our feedback page.

Malware Assessment data collection details

Malware Assessment collects configuration data, metadata, and state data using the agents that you have enabled.

The following table shows data collection methods and other details about how data is collected for Malware Assessment.

PLATFORM	DIRECT AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows	●	●	✗	✗	●	hourly

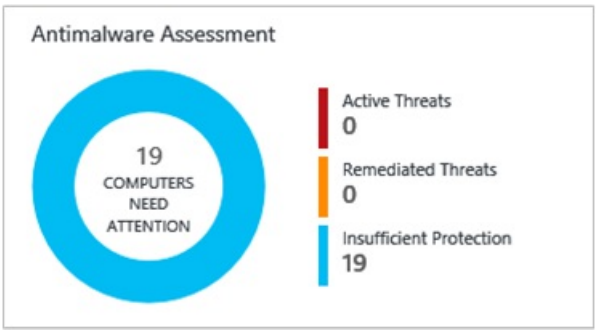
The following table shows examples of data types collected by Malware Assessment:

DATA TYPE	FIELDS
Configuration	CustomerID, AgentID, EntityID, ManagedTypeID, ManagedTypePropertyID, CurrentValue, ChangeDate
Metadata	BaseManagedEntityId, ObjectStatus, OrganizationalUnit, ActiveDirectoryObjectSid, PhysicalProcessors, NetworkName, IPAddress, ForestDNSName, NetbiosComputerName, VirtualMachineName, LastInventoryDate, HostServerNameIsVirtualMachine, IP Address, NetbiosDomainName, LogicalProcessors, DNSName, DisplayName, DomainDnsName, ActiveDirectorySite, PrincipalName, OffsetInMinuteFromGreenwichTime
State	StateChangeEventId, StateId, NewHealthState, OldHealthState, Context, TimeGenerated, TimeAdded, StateId2, BaseManagedEntityId, MonitorId, HealthState, LastModified, LastGreenAlertGenerated, DatabaseTimeModified

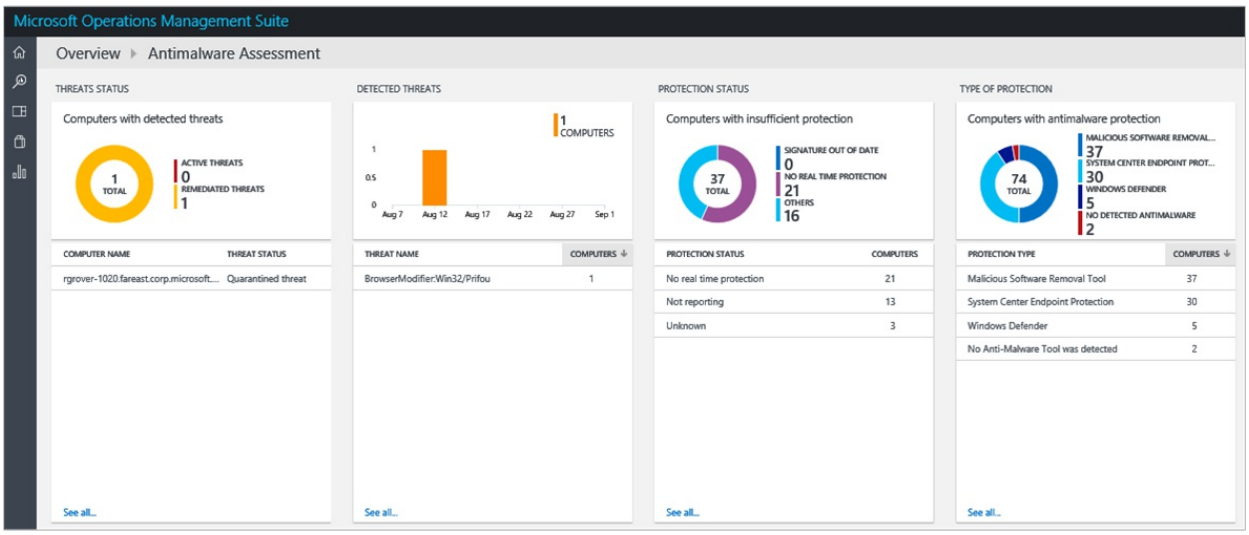
Review threats for servers

When your computers are adequately protected, active threats are quickly quarantined by your antimalware software and should rarely appear as active threats. For that reason, review remediated threats that show the effectiveness of the Antimalware Assessment solution in the following example procedure.

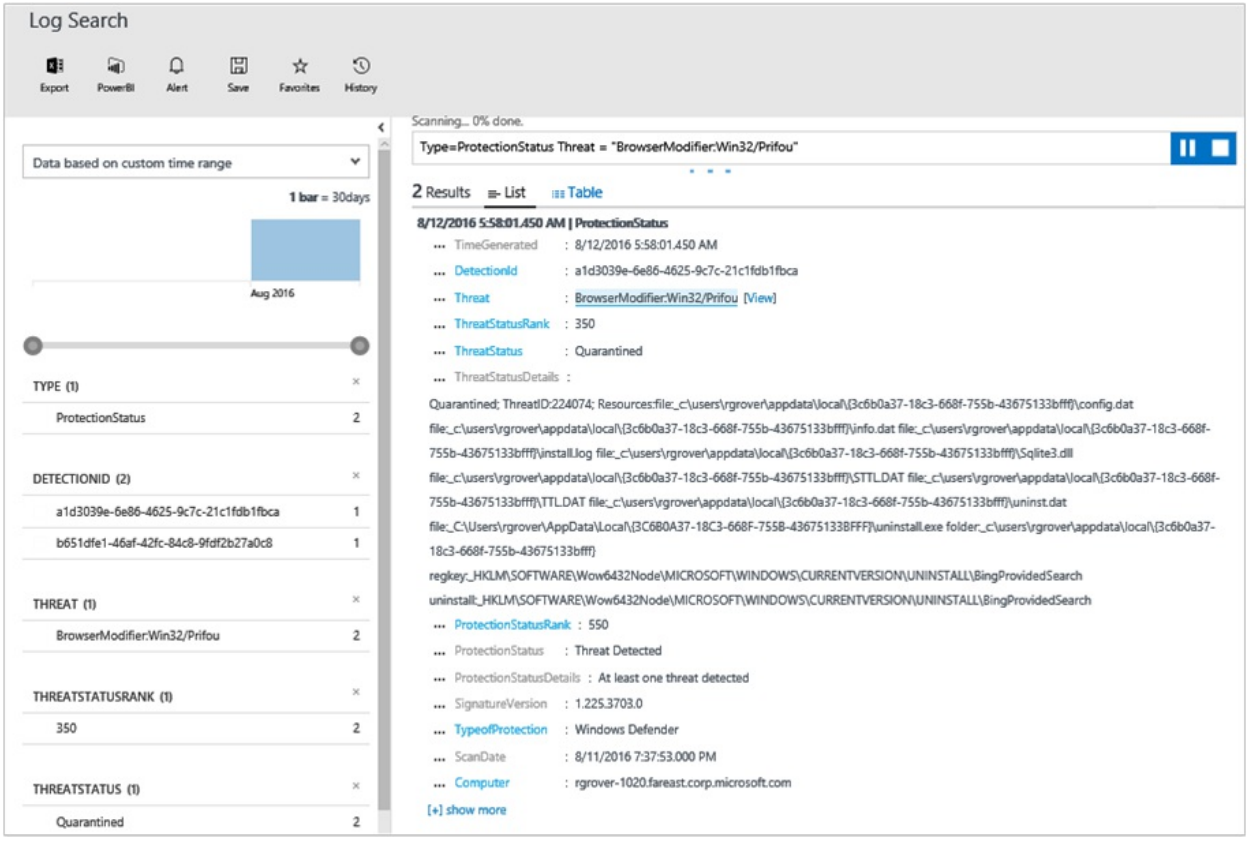
1. On the **Overview** page, click the **Antimalware Assessment** tile.



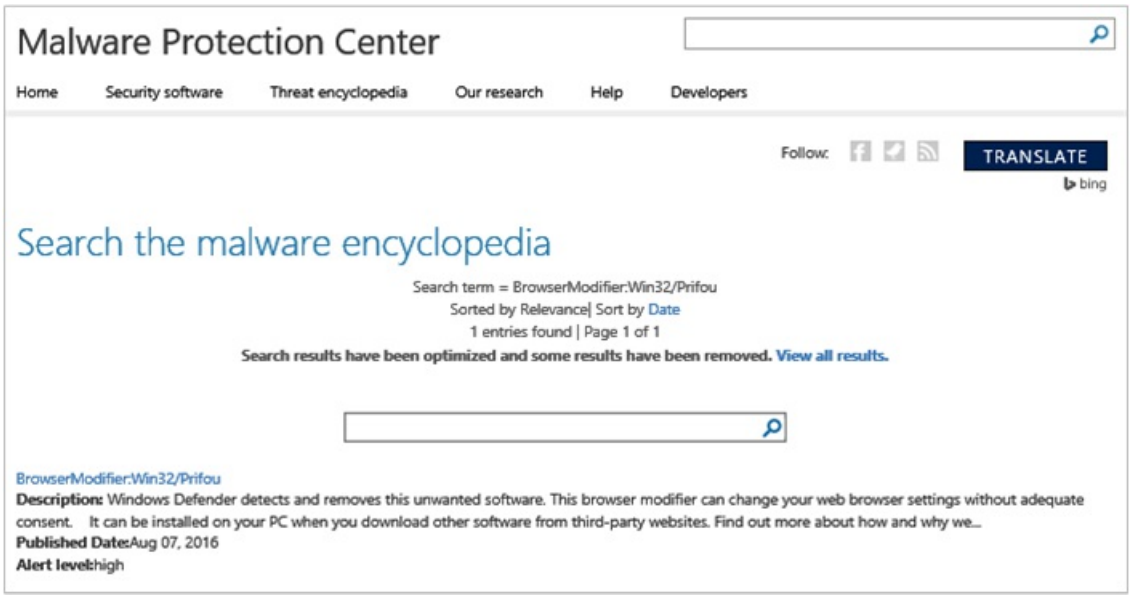
2. On the **Antimalware** dashboard, review the **Detected Threats** blade and click a server name with remediated threats.



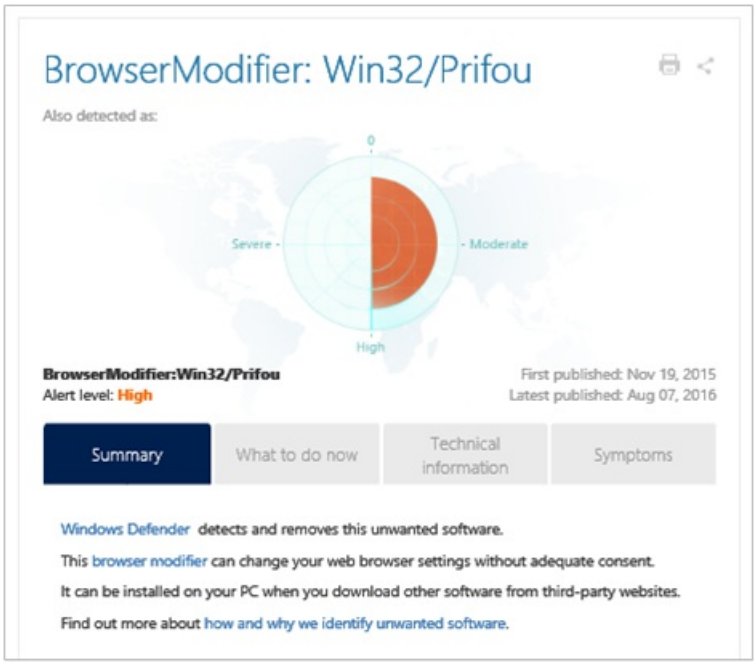
3. On the **Search** page you can see detailed information about the quarantined threat. Next to **Threat**, click **View**.



4. On the **Search the malware encyclopedia** page, click the malware item to view more details about it.

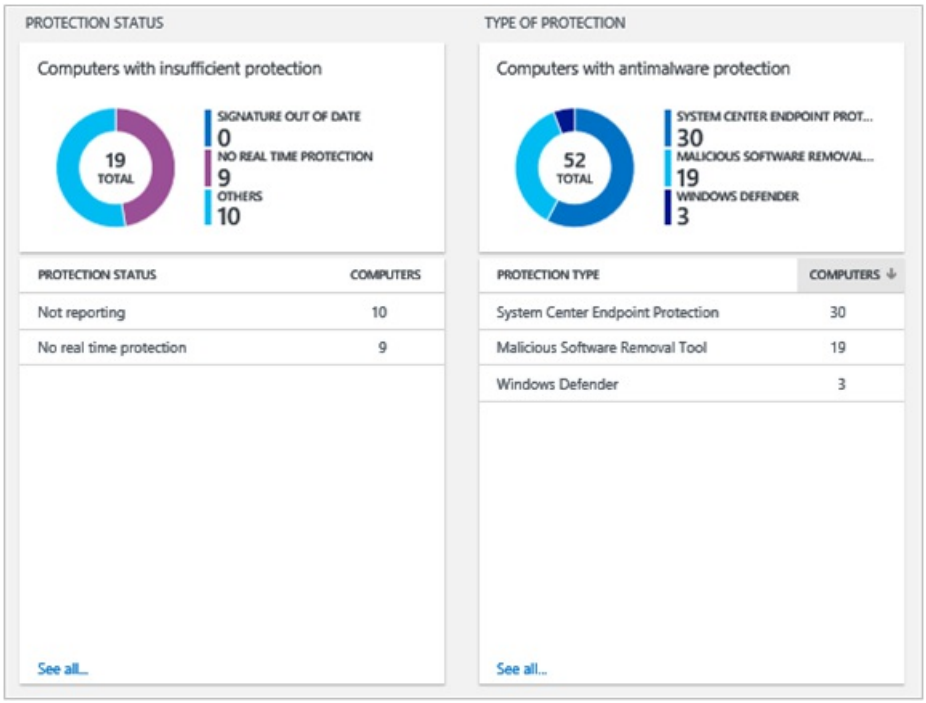


5. On the Microsoft **Malware Protection Center** page for the malware item, review information in the **Summary** section. This section describes how your antimalware software can detect and remove the threat and provides information about what threat the malware might have to your computers.

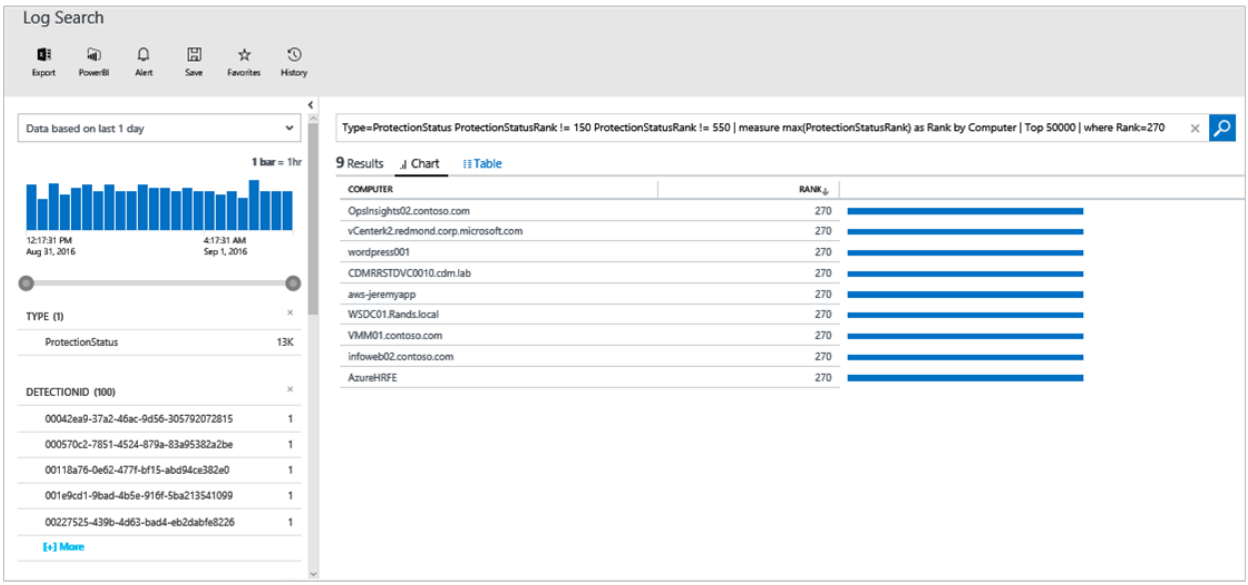


Review protection status

1. On the **Antimalware** dashboard, review the **Protection Status** blade and click **No real time protection**.



2. Search shows a list of servers without protection.



3. Servers without real time protection are displayed.

Computers that do not have supported antimalware software are reported as **No real time protection**.

Next steps

- Use Log searches in Log Analytics to view detailed malware assessment data.

1 min to read •

Connecting your security products to the Operations Management Suite (OMS) Security and Audit Solution

3/30/2017 • 3 min to read • Edit Online

This document helps you connect your security products into the OMS Security and Audit Solution. The following sources are supported:

- Common Event Format (CEF) events
- Cisco ASA events

What is CEF?

Common Event Format (CEF) is an industry standard format on top of Syslog messages, used by many security vendors to allow event interoperability among different platforms. OMS Security and Audit Solution support data ingestion using CEF, which enables you to connect your security products with OMS Security.

By connecting your data source to OMS, you are able to take advantage of the following capabilities that are part of this platform:

- Search & Correlation
- Auditing
- Alert
- Threat Intelligence
- Notable Issues

Collection of security solution logs

OMS Security supports collection of logs using CEF over Syslogs and Cisco ASA logs. In this example, the source (computer that generates the logs) is a Linux computer running syslog-ng daemon and the target is OMS Security. To prepare the Linux computer you will need to perform the following tasks:

- Download the OMS Agent for Linux, version 1.2.0-25 or above.
- Follow the section **Quick Install Guide** from this article to install and onboard the agent to your workspace.

Typically, the agent is installed on a different computer from the one on which the logs are generated. Forwarding the logs to the agent machine will usually require the following steps:

- Configure the logging product/machine to forward the required events to the syslog daemon (rsyslog or syslog-ng) on the agent machine.
- Enable the syslog daemon on the agent machine to receive messages from a remote system.

On the agent machine, the events need to be sent from the syslog daemon to local UDP port 25226. The agent is listening for incoming events on this port. The following is an example configuration for sending all events from the local system to the agent (you can modify the configuration to fit your local settings):

1. Open the terminal window, and go to the directory */etc/syslog-ng/*
2. Create a new file *security-config-omsagent.conf* and add the following content: OMS_facility = local4

   filter f_local4_oms { facility(local4); };

destination security_oms { tcp("127.0.0.1" port(25226)); };

log { source(src); filter(f_local4_oms); destination(security_oms); };

3. Download the file *security_events.conf* and place at */etc/opt/microsoft/omsagent/conf/omsagent.d/* in the OMS Agent computer.

4. Type the command below to restart the syslog daemon: *For syslog-ng run:*

```
sudo service rsyslog restart
```

For rsyslog run:

```
/etc/init.d/syslog-ng restart
```

5. Type the command below to restart the OMS Agent:

For syslog-ng run:

```
sudo service omsagent restart
```

For rsyslog run:

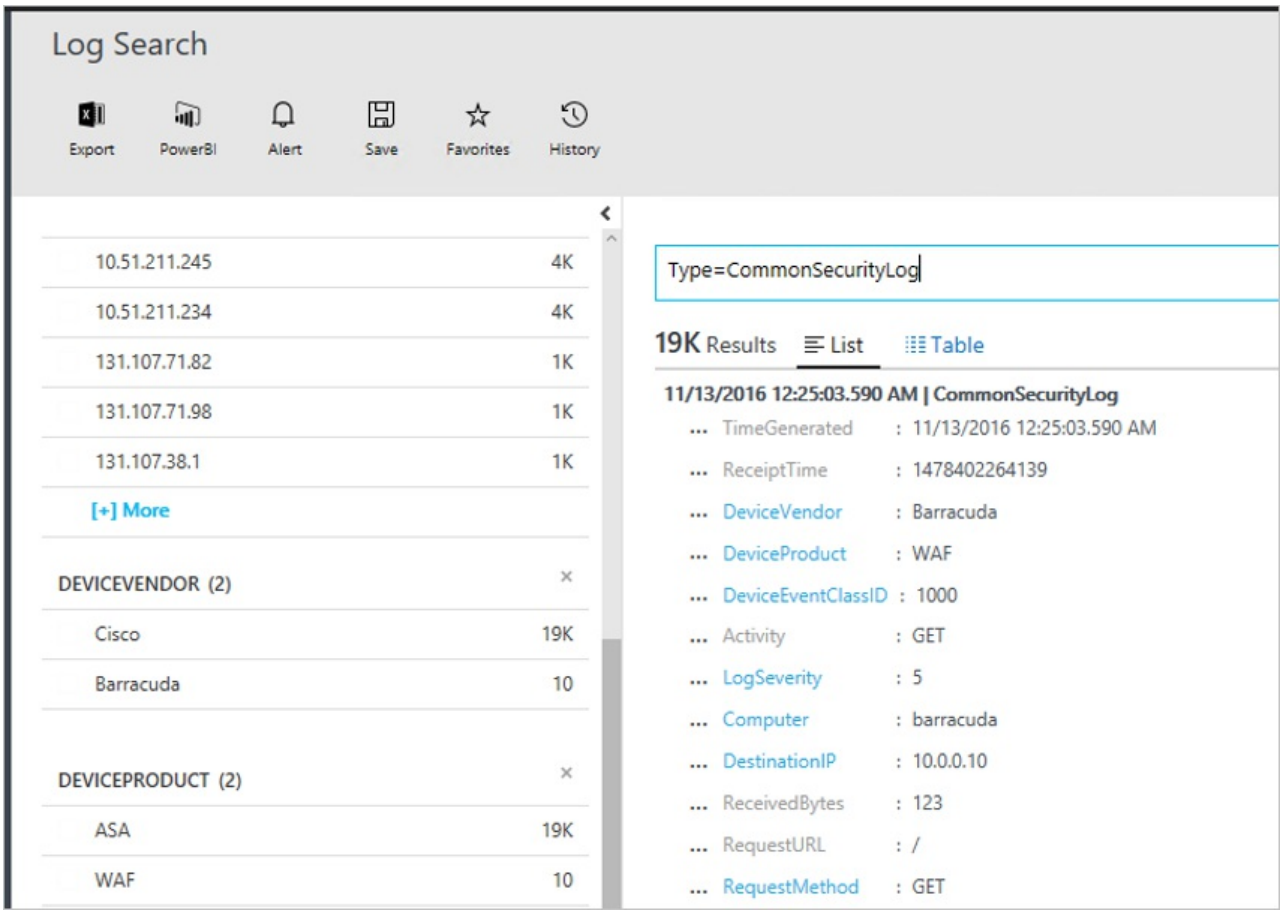
```
systemctl restart omsagent
```

6. Type the command below and review the result to confirm that there are no errors in the OMS Agent log:

```
tail /var/opt/microsoft/omsagent/log/omsagent.log
```

Reviewing collected security events

After the configuration is over, the security event will start to be ingested by OMS Security. To visualize those events, open the Log Search, type the command *Type=CommonSecurityLog* in the search field and press ENTER. The following example shows the result of this command, notice that in this case OMS Security already ingested security logs from multiple vendors:



You can refine this search for one single vendor, for example, to visualize online Cisco logs, type: *Type=CommonSecurityLog DeviceVendor=Cisco*. The "CommonSecurityLog" has predefined fields for any CEF header including the basic extensios, while any other extension whether it's "Custom Extension" or not, will be inserted into "AdditionalExtensions" field. You can use the Custom Fields feature to get dedicated fields from it.

Accessing computers missing baseline assessment

OMS supports the domain member baseline profile on Windows Server 2008 R2 up to Windows Server 2012 R2. Windows Server 2016 baseline isn't final yet and will be added as soon as it is published. All other operating systems scanned via OMS Security and Audit baseline assessment appear under the **Computers missing baseline assessment** section.

See also

In this document, you learned how to connect your CEF solution to OMS. To learn more about OMS Security, see the following articles:

- Operations Management Suite (OMS) overview
- Monitoring and Responding to Security Alerts in Operations Management Suite Security and Audit Solution
- Monitoring Resources in Operations Management Suite Security and Audit Solution

Working with management solutions in Operations Management Suite (OMS) (Preview)

3/21/2017 • 4 min to read • Edit Online

> **NOTE**
> This is preliminary documentation for management solutions in OMS which are currently in preview.

Management solutions extend the functionality of Operations Management Suite (OMS) by providing packaged management scenarios that customers can add to their environment. In addition to solutions provided by Microsoft, partners and customers can create management solutions to be used in their own environment or made available to customers through the community.

Finding and installing management solutions

There are multiple methods for locating and installing management solutions as described in the following sections.

Azure Marketplace

Management solutions provided by Microsoft and trusted partners may be installed from the Azure Marketplace in the Azure portal.

1. Log in to the Azure portal.
2. In the left pane, select **More services**.
3. Either scroll down to **Solutions** or type *solutions* into the **Filter** dialog.
4. Click the **+ Add** button.
5. Search for solutions that you're interested in either by browsing, clicking the **Filter** button, or typing in the **Search Everthing** box.
6. Click a marketplace item to view its detailed information.
7. Click **Create** to open the **Add Solution** pane.
8. You will be prompted to required information such as the OMS workspace and Automation account in addition to values for any parameters in the solution.
9. Click **Create** to install the solution.

OMS Portal

Management solutions provided by Microsoft may be installed from the Solutions Gallery in the OMS portal.

1. Log in to the OMS portal.
2. Click the **Solutions Gallery** tile.
3. On the OMS Solutions Gallery page, learn about each available solution. Click the name of the solution that you want to add to OMS.
4. On the page for the solution that you chose, detailed information about the solution is displayed. Click **Add**.
5. A new tile for the solution that you added appears on the Overview page in OMS and you can start using it after the OMS service processes your data.

Azure Quickstart Templates

Members of the community can submit management solutions to Azure Quickstart Templates. You can either

download these templates for later installation or inspect them to learn how to create your own solutions.

1. Follow the process described in OMS workspace and Automation account to link a workspace and account.
2. Go to Azure Quickstart Templates.
3. Search for a solution that you're interested in.
4. Select the solution from the results to view its details.
5. Click the **Deploy to Azure** button.
6. You will be prompted to provide information such as the resource group and location in addition to values for any parameters in the solution.
7. Click **Purchase** to install the solution.

Deploy Azure Resource Manager template

Solutions that you get from the community or that you create yourself are implemented as a Resource Manager template, and you can use any of the standard methods for deploying a template. Note that before installing the solution, you must create and link the OMS workspace and Automation account.

OMS workspace and Automation account

Most management solutions require an OMS workspace to contain views and an Automation account to contain runbooks and related resources. The workspace and account must meet the following requirements.

- A solution can only use one OMS workspace and one Automation account.
- The OMS workspace and Automation account used by a solution must be linked to one another. An OMS workspace may only be linked to one Automation account, and an Automation account may only be linked to one OMS workspace.
- To be linked, the OMS workspace and Automation account must be in the same resource group and region. The exception is an OMS workspace in East US region and and Automation account in East US 2.

Creating a link between an OMS workspace and Automation account

How you specify the OMS workspace and Automation account depends on the installation method for your solution.

- When you install a Microsoft solution through the OMS portal, it is installed in the current OMS workspace and no Automation account is required.
- When you install a solution through the Azure Marketplace, you are prompted for an OMS workspace and Automation account, and the link between them is created for you.
- For solutions outside of the Azure Marketplace, you must link the OMS workspace and Automation account before installing the solution. You can do this by selecting any solution in the Azure Marketplace and selecting the OMS workspace and Automation account. You don't have to actually install the solution because the link will be created as soon as the OMS workspace and Automation account are selected. Once the link is created, then you can use that OMS workspace and Automation account for any solution.

Verifying the link between an OMS workspace and Automation account

You can verify the link between an OMS workspace and an Automation account using the following procedure.

1. Select the Automation account in the Azure portal.
2. Scroll to the bottom of the **Settings** pane.
3. If there is a section called **OMS Resources** in the **Settings** pane, then this account is attached to an OMS workspace.
4. Select **Workspace** to view the details of the OMS workspace linked to this Automation account.

Listing management solutions

Use the following procedure to to view the management solutions in the workspaces linked to your Azure subscription.

1. Log in to the Azure portal.
2. In the left pane, select **More services**.
3. Either scroll down to **Solutions** or type *solutions* into the **Filter** dialog.
4. Solutions installed in all your workspaces will be listed.

Note that you can view only the Microsoft solutions installed in the current workspace using the OMS portal.

Removing a management solution

When a management solution is removed, all resources in the solution are also removed.

1. Locate the solution in the Azure portal using the procedure in Listing solutions.
2. Select the solution you want to remove.
3. Click the **Delete** button.

Creating a management solution

Complete guidance on creating management solutions are available at Creating solutions in Operations Management Suite (OMS).

Next steps

- Search Azure Quickstart Templates for samples of different Resource Manager templates.
- Create your own management solutions.

Use solution targeting in Operations Management Suite (OMS) to scope management solutions to specific agents (Preview)

4/27/2017 • 3 min to read • Edit Online

When you add a solution to OMS, it's automatically deployed by default to all Windows and Linux agents connected to your Log Analytics workspace. You may want to manage your costs and limit the amount of data collected for a solution by limiting it to a particular set of agents. This article describes how to use **Solution Targeting** which is an OMS feature that allows you to apply a scope to your solutions.

How to target a solution

There are three steps to targeting a solution as described in the following sections. Note that you will need both the OMS portal and the Azure portal for different steps.

1. Create a computer group

You specify the computers that you want to include in a scope by creating a computer group in Log Analytics. The computer group can be based on a log search or imported from other sources such as Active Directory or WSUS groups. As described below, only computers that are directly connected to Log Analytics will be included in the scope.

Once you have the computer group created in your workspace, then you'll include it in a scope configuration that can be applied to one or more solutions.

2. Create a scope configuration

A **Scope Configuration** includes one or more computer groups and can be applied to one or more solutions.

Create a scope configuration using the following process.

1. In the Azure portal, navigate to **Log Analytics** and select your workspace.
2. In the properties for the workspace under **Workspace Data Sources** select **Scope Configurations**.
3. Click **Add** to create a new scope configuration.
4. Type a **Name** for the scope configuration.
5. Click **Select Computer Groups**.
6. Select the computer group that you created and optionally any other groups to add to the configuration. Click **Select**.
7. Click **OK** to create the scope configuration.

3. Apply the scope configuration to a solution.

Once you have a scope configuration, then you can apply it to one or more solutions. Note that while a single scope configuration can be used with multiple solutions, each solution can only use one scope configuration.

Apply a scope configuration using the following process.

1. In the Azure portal, navigate to **Log Analytics** and select your workspace.
2. In the properties for the workspace select **Solutions**.
3. Click on the solution you want to scope.
4. In the properties for the solution under **Workspace Data Sources** select **Solution Targeting**. If the option is not available then this solution cannot be targeted.

5. Click **Add scope configuration**. If you already have a configuration applied to this solution then this option will be unavailable. You must remove the existing configuration before adding another one.
6. Click on the scope configuration that you created.
7. Watch the **Status** of the configuration to ensure that it shows **Succeeded**. If the status indicates an error, then click the ellipse to the right of the configuration and select **Edit scope configuration** to make changes.

Solutions and agents that can't be targeted

Following are the criteria for agents and solutions that can't be used with solution targeting.

- Solution targeting only applies to solutions that deploy to agents.
- Solution targeting only applies to solutions provided by Microsoft. It does not apply to solutions created by yourself or partners.
- You can only filter out agents that connect directly to Log Analytics. Solutions will automatically deploy to any agents that are part of a connected Operations Manager management group whether or not they're included in a scope configuration.

Exceptions

Solution targeting cannot be used with the following solutions even though they fit the stated criteria.

- Agent Health Assessment

Next steps

- Learn more about management solutions including the solutions that are available to install in your environment at Add Azure Log Analytics management solutions to your workspace.
- Learn more about creating computer groups at Computer groups in Log Analytics log searches.

Optimize your Active Directory environment with the Active Directory Assessment solution in Log Analytics

4/12/2017 • 7 min to read • Edit Online

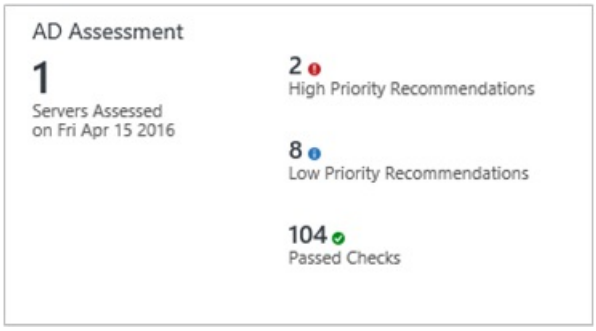
You can use the Active Directory Assessment solution to assess the risk and health of your server environments on a regular interval. This article will help you install and use the solution so that you can take corrective actions for potential problems.

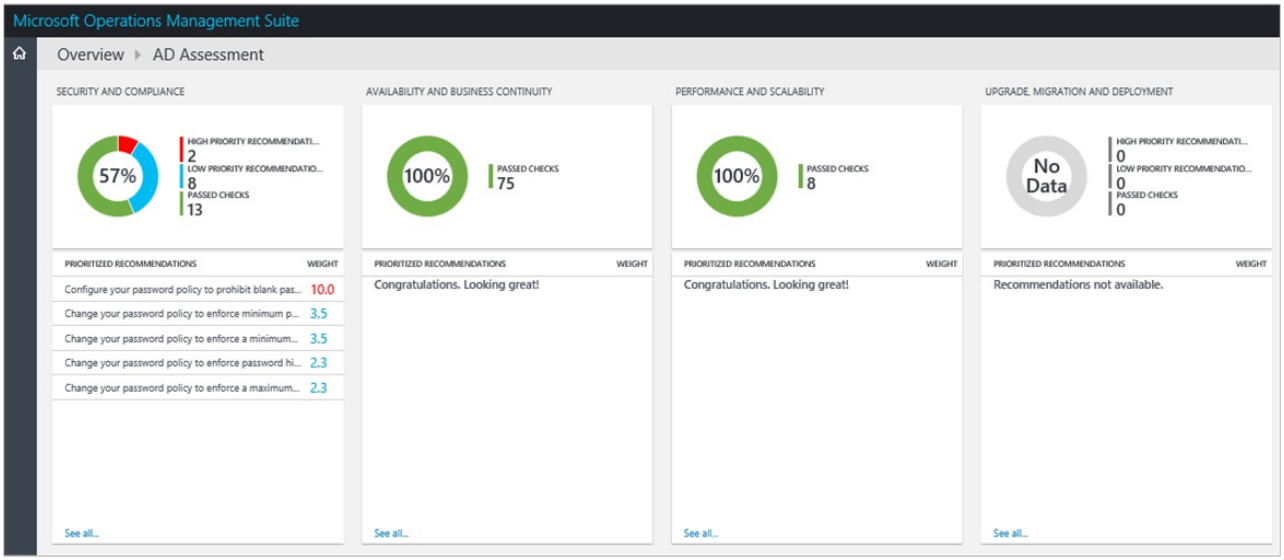
This solution provides a prioritized list of recommendations specific to your deployed server infrastructure. The recommendations are categorized across four focus areas which help you quickly understand the risk and take action.

The recommendations are based on the knowledge and experience gained by Microsoft engineers from thousands of customer visits. Each recommendation provides guidance about why an issue might matter to you and how to implement the suggested changes.

You can choose focus areas that are most important to your organization and track your progress toward running a risk free and healthy environment.

After you've added the solution and an assessment is completed, summary information for focus areas is shown on the **AD Assessment** dashboard for the infrastructure in your environment. The following sections describe how to use the information on the **AD Assessment** dashboard, where you can view and then take recommended actions for your Active Directory server infrastructure.





Installing and configuring the solution

Use the following information to install and configure the solutions.

- Agents must be installed on domain controllers that are members of the domain to be evaluated.
- The Active Directory Assessment solution requires a supported version of .NET Framework 4 (4.5.2 or above) installed on each computer that has an OMS agent.
- Add the Active Directory Assessment solution to your OMS workspace from Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery. There is no further configuration required.

> **NOTE**
> After you've added the solution, the AdvisorAssessment.exe file is added to servers with agents. Configuration data is read and then sent to the OMS service in the cloud for processing. Logic is applied to the received data and the cloud service records the data.

Active Directory Assessment data collection details

Active Directory Assessment collects WMI data, registry data, and performance data using the agents that you have enabled.

The following table shows data collection methods for agents, whether Operations Manager (SCOM) is required, and how often data is collected by an agent.

PLATFORM	DIRECT AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows						7 days

Understanding how recommendations are prioritized

Every recommendation made is given a weighting value that identifies the relative importance of the recommendation. Only the ten most important recommendations are shown.

How weights are calculated

Weightings are aggregate values based on three key factors:

- The *probability* that an issue identified will cause problems. A higher probability equates to a larger overall score for the recommendation.
- The *impact* of the issue on your organization if it does cause a problem. A higher impact equates to a larger overall score for the recommendation.
- The *effort* required to implement the recommendation. A higher effort equates to a smaller overall score for the recommendation.

The weighting for each recommendation is expressed as a percentage of the total score available for each focus area. For example, if a recommendation in the Security and Compliance focus area has a score of 5%, implementing that recommendation will increase your overall Security and Compliance score by 5%.

Focus areas

Security and Compliance - This focus area shows recommendations for potential security threats and breaches, corporate policies, and technical, legal and regulatory compliance requirements.

Availability and Business Continuity - This focus area shows recommendations for service availability, resiliency

of your infrastructure, and business protection.

Performance and Scalability - This focus area shows recommendations to help your organization's IT infrastructure grow, ensure that your IT environment meets current performance requirements, and is able to respond to changing infrastructure needs.

Upgrade, Migration and Deployment - This focus area shows recommendations to help you upgrade, migrate, and deploy Active Directory to your existing infrastructure.

Should you aim to score 100% in every focus area?

Not necessarily. The recommendations are based on the knowledge and experiences gained by Microsoft engineers across thousands of customer visits. However, no two server infrastructures are the same, and specific recommendations may be more or less relevant to you. For example, some security recommendations might be less relevant if your virtual machines are not exposed to the Internet. Some availability recommendations may be less relevant for services that provide low priority ad hoc data collection and reporting. Issues that are important to a mature business may be less important to a start-up. You may want to identify which focus areas are your priorities and then look at how your scores change over time.

Every recommendation includes guidance about why it is important. You should use this guidance to evaluate whether implementing the recommendation is appropriate for you, given the nature of your IT services and the business needs of your organization.

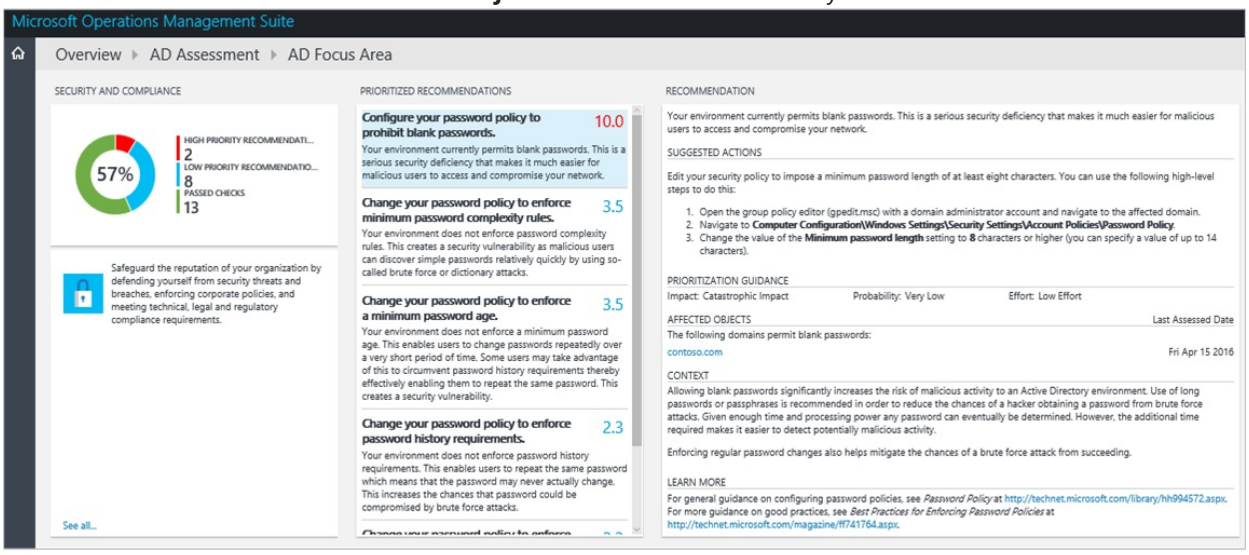
Use assessment focus area recommendations

Before you can use an assessment solution in OMS, you must have the solution installed. To read more about installing solutions, see Add Log Analytics solutions from the Solutions Gallery. After it is installed, you can view the summary of recommendations by using the Assessment tile on the Overview page in OMS.

View the summarized compliance assessments for your infrastructure and then drill-into recommendations.

To view recommendations for a focus area and take corrective action

1. On the **Overview** page, click the **Assessment** tile for your server infrastructure.
2. On the **Assessment** page, review the summary information in one of the focus area blades and then click one to view recommendations for that focus area.
3. On any of the focus area pages, you can view the prioritized recommendations made for your environment. Click a recommendation under **Affected Objects** to view details about why the recommendation is made.



4. You can take corrective actions suggested in **Suggested Actions**. When the item has been addressed, later assessments will record that recommended actions were taken and your compliance score will increase. Corrected items appear as **Passed Objects**.

Ignore recommendations

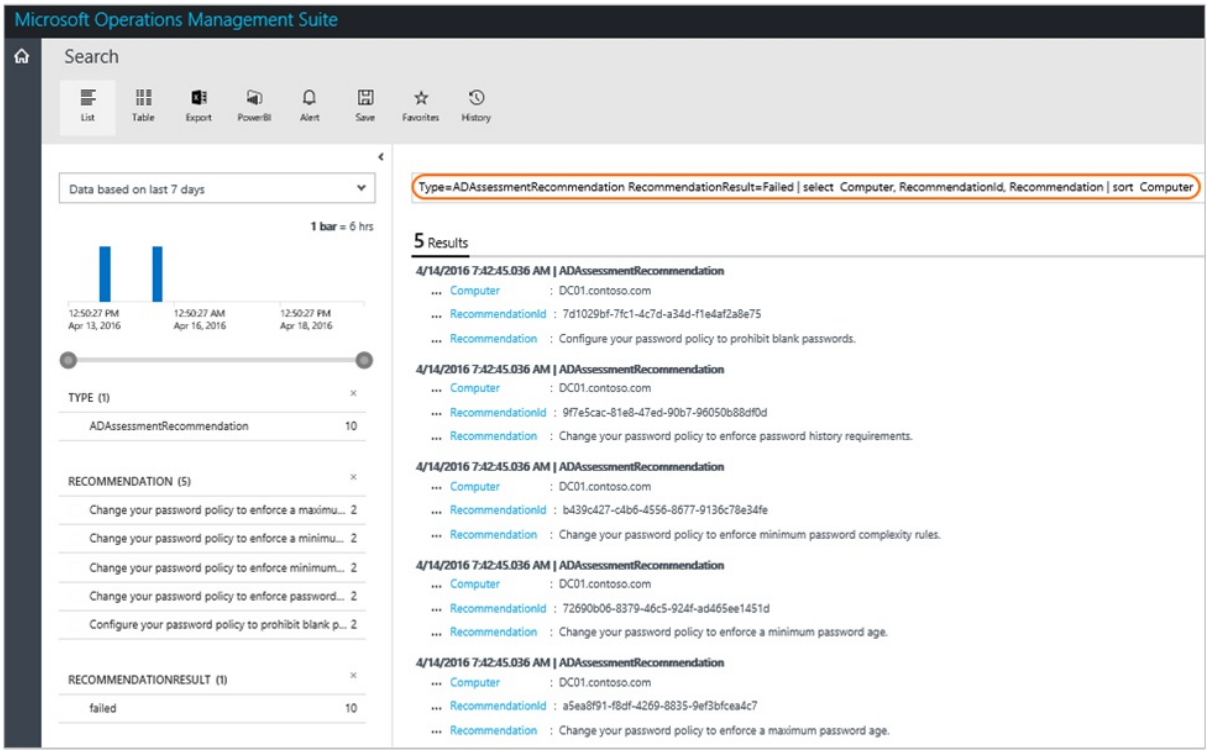
If you have recommendations that you want to ignore, you can create a text file that OMS will use to prevent recommendations from appearing in your assessment results.

To identify recommendations that you will ignore

1. Sign in to your workspace and open Log Search. Use the following query to list recommendations that have failed for computers in your environment.

   ```
   Type=ADAssessmentRecommendation RecommendationResult=Failed | select  Computer, RecommendationId, Recommendation | sort  Computer
   ```

   Here's a screen shot showing the Log Search query:

2. Choose recommendations that you want to ignore. You'll use the values for RecommendationId in the next procedure.

To create and use an IgnoreRecommendations.txt text file

1. Create a file named IgnoreRecommendations.txt.
2. Paste or type each RecommendationId for each recommendation that you want Log Analytics to ignore on a separate line and then save and close the file.
3. Put the file in the following folder on each computer where you want OMS to ignore recommendations.
   - On computers with the Microsoft Monitoring Agent (connected directly or through Operations Manager) - *SystemDrive*:\Program Files\Microsoft Monitoring Agent\Agent
   - On the Operations Manager management server - *SystemDrive*:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server

To verify that recommendations are ignored

After the next scheduled assessment runs, by default every 7 days, the specified recommendations are marked *Ignored* and will not appear on the assessment dashboard.

1. You can use the following Log Search queries to list all the ignored recommendations.

```
Type=ADAssessmentRecommendation RecommendationResult=Ignored | select  Computer, RecommendationId,
Recommendation | sort  Computer
```

2. If you decide later that you want to see ignored recommendations, remove any IgnoreRecommendations.txt files, or you can remove RecommendationIDs from them.

AD Assessment solutions FAQ

How often does an assessment run?

- The assessment runs every 7 days.

Is there a way to configure how often the assessment runs?

- Not at this time.

If another server for is discovered after I've added an assessment solution, will it be assessed?

- Yes, once it is discovered it is assessed from then on, every 7 days.

If a server is decommissioned, when will it be removed from the assessment?

- If a server does not submit data for 3 weeks, it is removed.

What is the name of the process that does the data collection?

- AdvisorAssessment.exe

How long does it take for data to be collected?

- The actual data collection on the server takes about 1 hour. It may take longer on servers that have a large number of Active Directory servers.

What type of data is collected?

- The following types of data are collected:
  - WMI
  - Registry
  - Performance counters

Is there a way to configure when data is collected?

- Not at this time.

Why display only the top 10 recommendations?

- Instead of giving you an exhaustive overwhelming list of tasks, we recommend that you focus on addressing the prioritized recommendations first. After you address them, additional recommendations will become available. If you prefer to see the detailed list, you can view all recommendations using Log Search.

Is there a way to ignore a recommendation?

- Yes, see Ignore recommendations section above.

Next steps

- Use Log searches in Log Analytics to view detailed AD Assessment data and recommendations.

Monitor Active Directory replication status with Log Analytics

4/12/2017 • 7 min to read • Edit Online

Active Directory is a key component of an enterprise IT environment. To ensure high availability and high performance, each domain controller has its own copy of the Active Directory database. Domain controllers replicate with each other in order to propagate changes across the enterprise. Failures in this replication process can cause a variety of problems across the enterprise.

The AD Replication Status solution pack regularly monitors your Active Directory environment for any replication failures and reports the results on your OMS dashboard.

Installing and configuring the solution

Use the following information to install and configure the solution.

- Agents must be installed on domain controllers that are members of the domain to be evaluated, or on member servers configured to send AD replication data to OMS. To understand how to connect Windows computers to OMS, see Connect Windows computers to Log Analytics. If your domain controller is already part of an existing System Center Operations Manager environment that you'd like to connect to OMS, see Connect Operations Manager to Log Analytics.
- Add the Active Directory Replication Status solution to your OMS workspace using the process described in Add Log Analytics solutions from the Solutions Gallery. There is no further configuration required.

AD Replication Status data collection details

The following table shows data collection methods and other details about how data is collected for AD Replication Status.

PLATFORM	DIRECT AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows						every 5 days

Optionally, enable a non-domain controller to send AD data to OMS

If you don't want to connect any of your domain controllers directly to OMS, you can use any other OMS-connected computer in your domain to collect data for the AD Replication Status solution pack and have it send the data.

To enable a non-domain controller to send AD data to OMS

1. Verify that the computer is a member of the domain that you wish to monitor using the AD Replication Status solution.
2. Connect the Windows computer to OMS or connect it using your existing Operations Manager environment to OMS, if it is not already connected.
3. On that computer, set the following registry key:

   - Key: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HealthService\Parameters\Management**

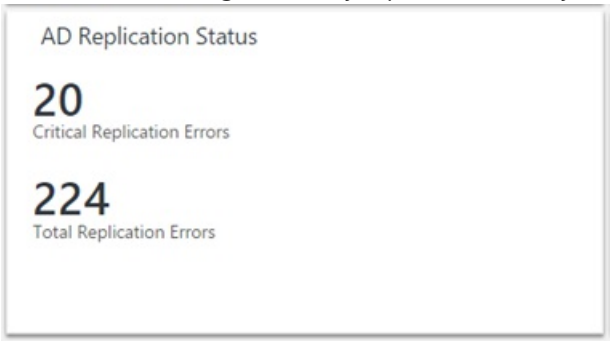
Groups<ManagementGroupName>\Solutions\ADReplication

- Value: **IsTarget**
- Value Data: **true**

> **NOTE**
> These changes will not take effect until your restart the Microsoft Monitoring Agent service (HealthService.exe).

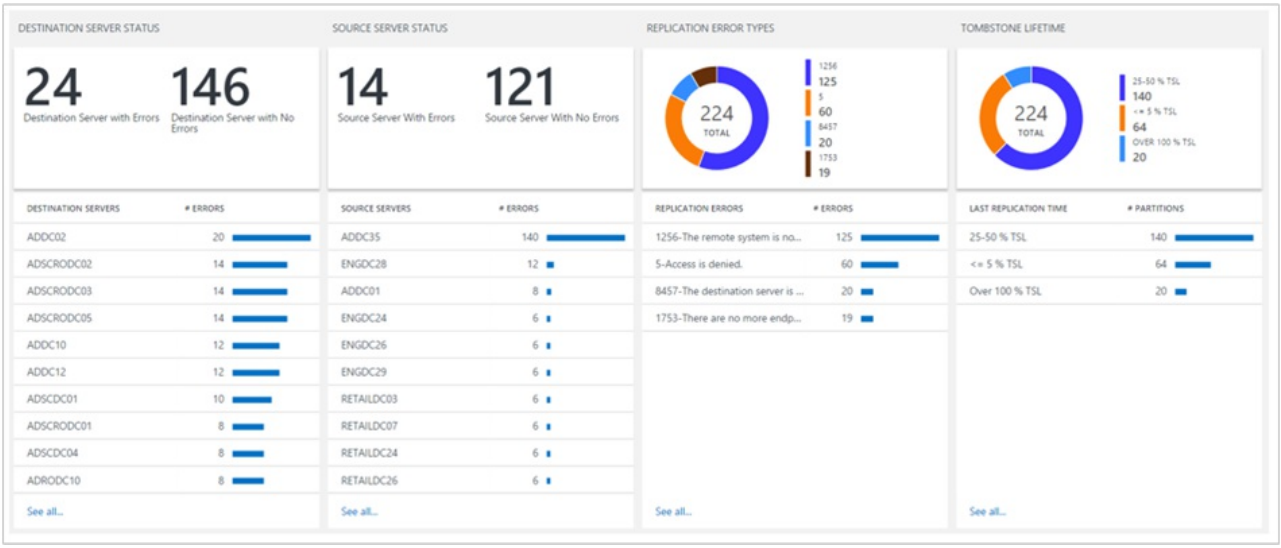
Understanding replication errors

Once you have AD replication status data sent to OMS, you'll see a tile similar to the following on the OMS dashboard indicating how many replication errors you currently have.



Critical Replication Errors are those that are at or above 75% of the tombstone lifetime for your Active Directory forest.

When you click the tile, you'll see more information about the errors.



Destination Server Status and Source Server Status

These blades show the status of destination servers and source servers that are experiencing replication errors. The number after each domain controller name indicates the number of replication errors on that domain controller.

The errors for both destination servers and source servers are shown because some problems are easier to troubleshoot from the source server perspective and others from the destination server perspective.

In this example, you can see that many destination servers have roughly the same number of errors, but there's one source server (ADDC35) that has many more errors than all the others. It's likely that there is some problem on ADDC35 that is causing it to fail to send data to its replication partners. Fixing the problems on ADDC35 will likely resolve many of the errors that appear in the destination server blade.

Replication Error Types

This blade gives you information about the types of errors detected throughout your enterprise. Each error has a unique numerical code and a message that can help you determine the root cause of the error.

The donut at the top gives you an idea of which errors appear more and less frequently in your environment.

This can show you when multiple domain controllers experience the same replication error. In this case, you may be able to discover identify a solution on one domain controller, then repeat it on other domain controllers affected by the same error.

Tombstone Lifetime

The tombstone lifetime determines how long a deleted object, referred to as a tombstone, is retained in the Active Directory database. When a deleted object passes the tombstone lifetime, a garbage collection process automatically removes it from the Active Directory database.

The default tombstone lifetime is 180 days for most recent versions of Windows, but it was 60 days on older versions, and it can be changed explicitly by an Active Directory administrator.

It's important to know if you're having replication errors that are approaching or are past the tombstone lifetime. If two domain controllers experience a replication error that persists past the tombstone lifetime, replication will be disabled between those two domain controllers, even if the underlying replication error is fixed.

The Tombstone Lifetime blade helps you identify places where this is in danger of happening. Each error in the **Over 100% TSL** category represents a partition that has not replicated between its source and destination server for at least the tombstone lifetime for the forest.

In this situation, simply fixing the replication error will not be enough. At a minimum, you'll need to manually investigate to identify and clean-up lingering objects before you can restart replication. You may even need to decommission a domain controller.

In addition to identifying any replication errors that have persisted past the tombstone lifetime, you'll also want to pay attention to any errors falling into the **50-75% TSL** or **75-100% TSL** categories.

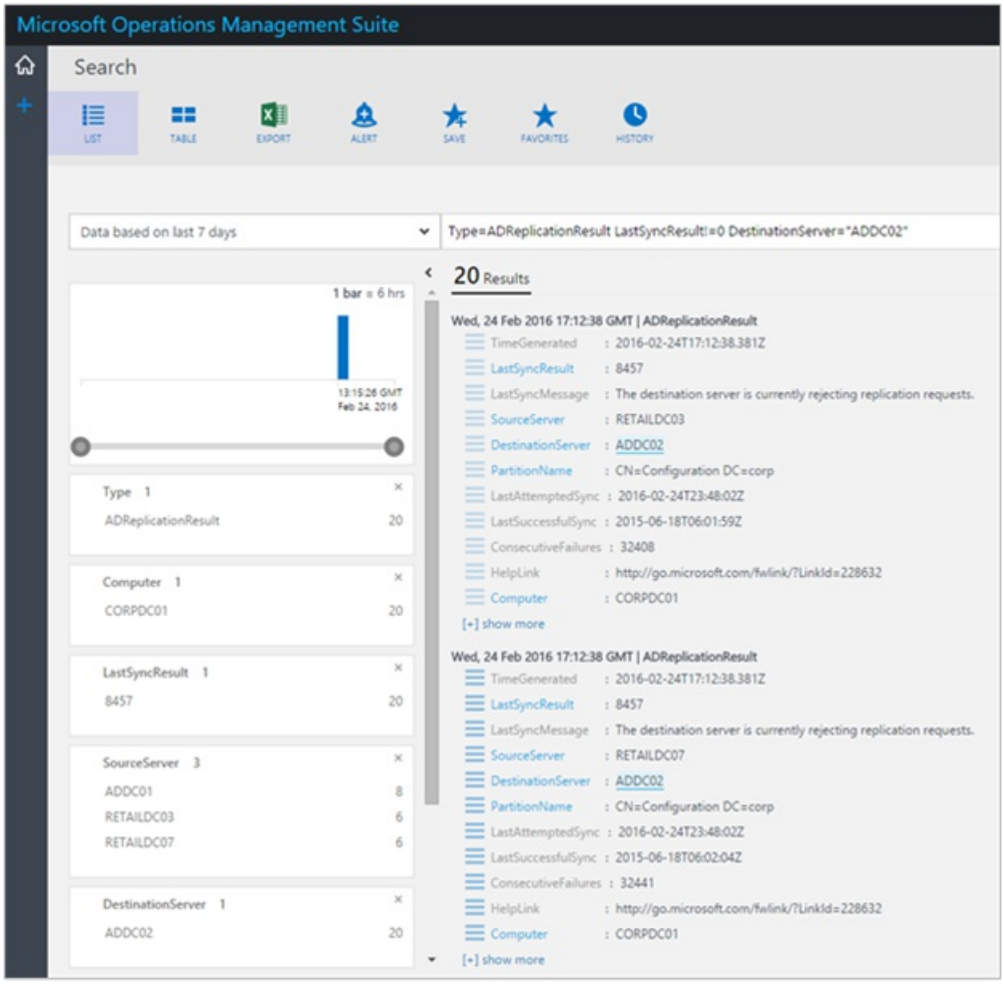
These are errors that are clearly lingering, not transient, so they likely need your intervention to resolve. The good news is that they have not yet reached the tombstone lifetime. If you fix these problems promptly and *before* they reach the tombstone lifetime, replication can restart with minimal manual intervention.

As noted earlier, the dashboard tile for the AD Replication Status solution shows the number of *critical* replication errors in your environment, which is defined as errors that are over 75% of tombstone lifetime (including errors that are over 100% of TSL). Strive to keep this number at 0.

> **NOTE**
>
> All the tombstone lifetime percentage calculations are based on the actual tombstone lifetime for your Active Directory forest, so you can trust that those percentages are accurate, even if you have a custom tombstone lifetime value set.

AD Replication status details

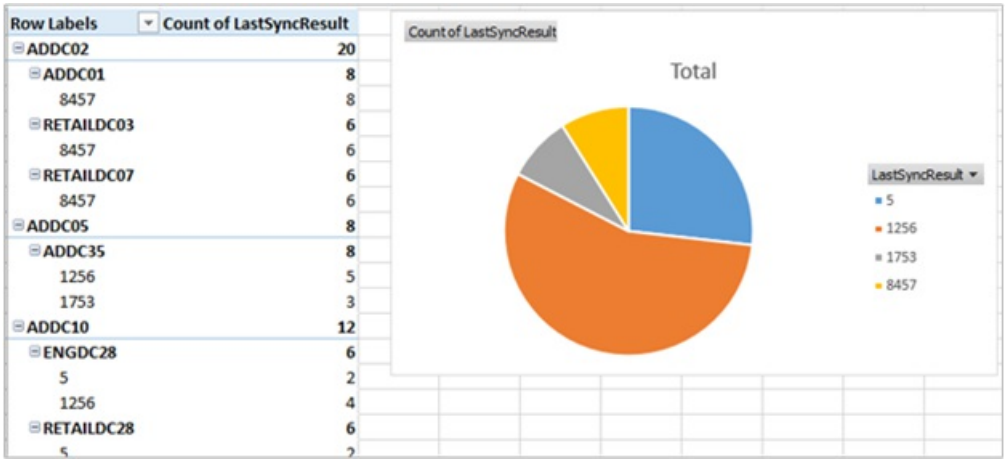
When you click any item in one of the lists, you'll see additional details about it using Log Search. The results are filtered to show only the errors related to that item. For example, if you click on the first domain controller listed under **Destination Server Status (ADDC02)**, you'll see search results filtered to show errors with that domain controller listed as the destination server:



From here, you can filter further, modify the search query, and so on. For more information about using the Log Search, see Log searches.

The **HelpLink** field shows the URL of a TechNet page with additional details about that specific error. You can copy and paste this link into your browser window to see information about troubleshooting and fixing the error.

You can also click **Export** to export the results to Excel. This allows you to visualize replication error data in any way you'd like.



AD Replication Status FAQ

Q: How often is AD replication status data updated? A: The information is updated every 5 days.

Q: Is there a way to configure how often this data is updated? A: Not at this time.

Q: Do I need to add all of my domain controllers to my OMS workspace in order to see replication status?

A: No, only a single domain controller must be added. If you have multiple domain controllers in your OMS workspace, data from all of them is sent to OMS.

Q: I don't want to add any domain controllers to my OMS workspace. Can I still use the AD Replication Status solution? A: Yes. You can set the value of a registry key to enable this. See To enable a non-domain controller to send AD data to OMS.

Q: What is the name of the process that does the data collection? A: AdvisorAssessment.exe

Q: How long does it take for data to be collected? A: Data collection time depends on the size of the Active Directory environment, but usually takes less than 15 minutes.

Q: What type of data is collected? A: Replication information is collected via LDAP.

Q: Is there a way to configure when data is collected? A: Not at this time.

Q: What permissions do I need to collect data? A: Normal user permissions to Active Directory are usually sufficient.

Troubleshoot data collection problems

In order to collect data, the AD Replication Status solution pack requires at least one domain controller to be connected to your OMS workspace. Until you do this, you will see a message indicating that **data is still being collected**.

If you need assistance connecting one of your domain controllers, you can view documentation at Connect Windows computers to Log Analytics. Alternatively, if your domain controller is already connected to an existing System Center Operations Manager environment, you can view documentation at Connect System Center Operations Manager to Log Analytics.

If you don't want to connect any of your domain controllers directly to OMS or to SCOM, see To enable a non-domain controller to send AD data to OMS.

Next steps

- Use Log searches in Log Analytics to view detailed Active Directory Replication status data.

Alert Management solution in Operations Management Suite (OMS)

3/8/2017 • 5 min to read • Edit Online

The Alert Management solution helps you analyze all of the alerts in your Log Analytics repository. These alerts may have come from a variety of sources including those created by Log Analytics or imported from Nagios or Zabbix. The solution also imports alerts from any connected System Center Operations Manager (SCOM) management groups.

Prerequisites

The solution will work with any records in the Log Analytics repository with a type of **Alert**, so you must perform whatever configuration is required to collect these records.

- For Log Analytics alerts, create alert rules to create alert records directly in the repository.
- For Nagios and Zabbix alerts, configure those servers to send alerts to Log Analytics.
- For SCOM alerts,connect your Operations Manager management group to your Log Analytics workspace. Any alerts created in SCOM will be imported into Log Analytics.

Configuration

Add the Alert Management solution to your OMS workspace using the process described in Add solutions. There is no further configuration required.

Management packs

If your SCOM management group is connected to your OMS workspace, then the following management packs will be installed in SCOM when you add this solution. There is no configuration or maintenance of these management packs required.

- Microsoft System Center Advisor Alert Management (Microsoft.IntelligencePacks.AlertManagement)

For more information on how solution management packs are updated, see Connect Operations Manager to Log Analytics.

Data collection

Agents

The following table describes the connected sources that are supported by this solution.

CONNECTED SOURCE	SUPPORT	DESCRIPTION

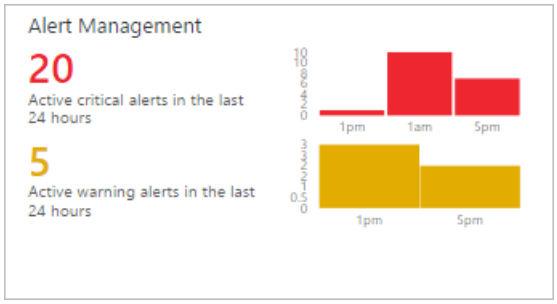
CONNECTED SOURCE	SUPPORT	DESCRIPTION
Windows agents	No	Direct Windows agents do not generate alerts. Log Analytics alerts can be created from events and performance data collected from Windows agents.
Linux agents	No	Direct Linux agents do not generate alerts. Log Analytics alerts can be created from events and performance data collected from Linux agents. Nagios and Zabbix alerts are collected from those servers which require the Linux agent.
SCOM management group	Yes	Alerts that are generated on SCOM agents are delivered to the management group and then forwarded to Log Analytics. A direct connection from SCOM agents to Log Analytics is not required. Alert data is forwarded from the management group to the Log Analytics repository.

Collection frequency

- Alert records are available to the solution as soon as they are stored in the repository.
- Alert data is sent from the SCOM management group to Log Analytics every 3 minutes.

Using the solution

When you add the Alert Management solution to your OMS workspace, the **Alert Management** tile will be added to your OMS dashboard. This tile displays a count and graphical representation of the number of currently active alerts that were generated within the last 24 hours. You cannot change this time range.

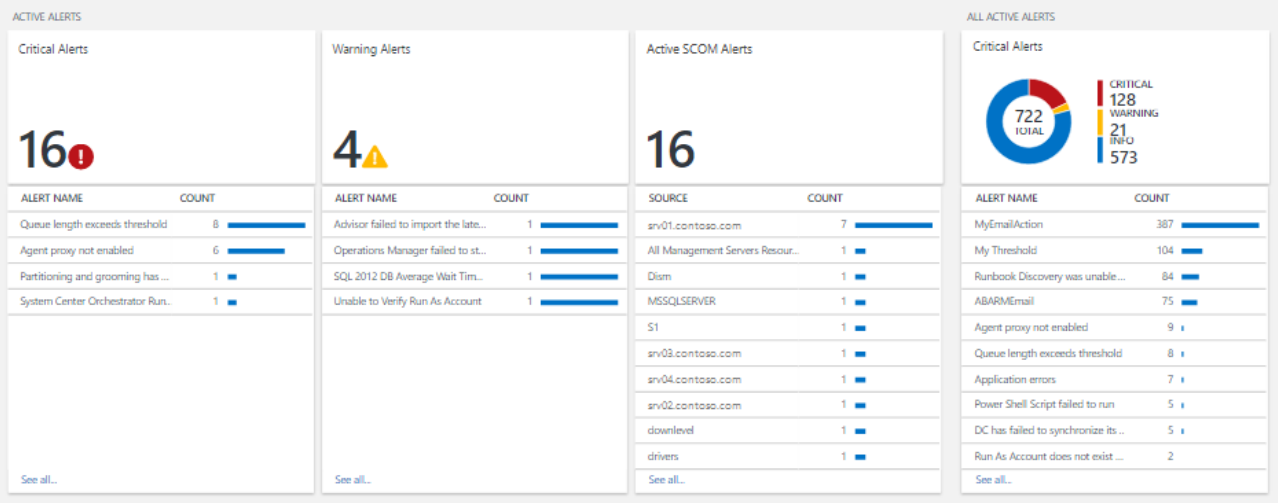


Click on the **Alert Management** tile to open the **Alert Management** dashboard. The dashboard includes the columns in the following table. Each column lists the top ten alerts by count matching that column's criteria for the specified scope and time range. You can run a log search that provides the entire list by clicking **See all** at the bottom of the column or by clicking the column header.

COLUMN	DESCRIPTION
Critical Alerts	All alerts with a severity of Critical grouped by alert name. Click on an alert name to run a log search returning all records for that alert.

COLUMN	DESCRIPTION
Warning Alerts	All alerts with a severity of Warning grouped by alert name. Click on an alert name to run a log search returning all records for that alert.
Active SCOM Alerts	All alerts collected from SCOM with any state other than *Closed* grouped by source that generated the alert.
All Active Alerts	All alerts with any severity grouped by alert name. Only includes SCOM alerts with any state other than *Closed*.

If you scroll to the right, the dashboard will list several common queries that you can click on to perform a log search for alert data.



Log Analytics records

The Alert Management solution analyzes any record with a type of **Alert**. Alerts created by Log Analytics or collected from Nagios or Zabbix are not directly collected by the solution.

The solution does import alerts from SCOM and creates a corresponding record for each with a type of **Alert** and a SourceSystem of **OpsManager**. These records have the properties in the following table.

PROPERTY	DESCRIPTION
Type	*Alert*
SourceSystem	*OpsManager*
AlertContext	Details of the data item that caused the alert to be generated in XML format.
AlertDescription	Detailed description of the alert.
AlertId	GUID of the alert.
AlertName	Name of the alert.
AlertPriority	Priority level of the alert.

PROPERTY	DESCRIPTION
AlertSeverity	Severity level of the alert.
AlertState	Latest resolution state of the alert.
LastModifiedBy	Name of the user who last modified the alert.
ManagementGroupName	Name of the management group where the alert was generated.
RepeatCount	Number of time the same alert was generated for the same monitored object since being resolved.
ResolvedBy	Name of the user who resolved the alert. Empty if the alert has not yet been resolved.
SourceDisplayName	Display name of the monitoring object that generated the alert.
SourceFullName	Full name of the monitoring object that generated the alert.
TicketId	Ticket ID for the alert if the SCOM environment is integrated with a process for assigning tickets for alerts. Empty of no ticket ID is assigned.
TimeGenerated	Date and time that the alert was created.
TimeLastModified	Date and time that the alert was last changed.
TimeRaised	Date and time that the alert was generated.
TimeResolved	Date and time that the alert was resolved. Empty if the alert has not yet been resolved.

Sample log searches

The following table provides sample log searches for alert records collected by this solution.

QUERY	DESCRIPTION
Type=Alert SourceSystem=OpsManager AlertSeverity=error TimeRaised>NOW-24HOUR	Critical alerts raised during the past 24 hours
Type=Alert AlertSeverity=warning TimeRaised>NOW-24HOUR	Warning alerts raised during the past 24 hours
Type=Alert SourceSystem=OpsManager AlertState!=Closed TimeRaised>NOW-24HOUR | measure count() as Count by SourceDisplayName	Sources with active alerts raised during the past 24 hours
Type=Alert SourceSystem=OpsManager AlertSeverity=error TimeRaised>NOW-24HOUR AlertState!=Closed	Critical alerts raised during the past 24 hours which are still active

QUERY	DESCRIPTION
Type=Alert SourceSystem=OpsManager TimeRaised>NOW-24HOUR AlertState=Closed	Alerts raised during the past 24 hours which are now closed
Type=Alert SourceSystem=OpsManager TimeRaised>NOW-1DAY | measure count() as Count by AlertSeverity	Alerts raised during the past 1 day grouped by their severity
Type=Alert SourceSystem=OpsManager TimeRaised>NOW-1DAY | sort RepeatCount desc	Alerts raised during the past 1 day sorted by their repeat count value

Next steps

- Learn about Alerts in Log Analytics for details on generating alerts from Log Analytics.

Using Service Map solution in Operations Management Suite (OMS)

3/17/2017 • 13 min to read • Edit Online

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. It allows you to view your servers as you think of them – as interconnected systems that deliver critical services. Service Map shows connections between servers, processes, and ports across any TCP-connected architecture with no configuration required other than installation of an agent.

This article describes the details of using Service Map. For information on configuring Service Map and onboarding agents, see Configuring Service Map solution in Operations Management Suite (OMS)

Use cases: Make your IT processes dependency aware

Discovery

Service Map automatically builds a common reference map of dependencies across your servers, processes, and third-party services. It discovers and maps all TCP dependencies, identifying surprise connections, remote third-party systems you depend on, and dependencies to traditional dark areas of your network such as Active Directory. Service Map discovers failed network connections that your managed systems are attempting to make, helping you identify potential server misconfiguration, service outages, and network issues.

Incident management

Service Map helps eliminate the guesswork of problem isolation by showing you how systems are connected and affecting each other. In addition to failed connections, information about connected clients helps identify misconfigured load balancers, surprising or excessive load on critical services, and rogue clients such as developer machines talking to production systems. Integrated workflows with OMS Change Tracking also allow you to see whether a change event on a back-end machine or service explains the root cause of an incident.

Migration assurance

Service Map allows you to effectively plan, accelerate, and validate Azure migrations, ensuring that nothing is left behind and there are no surprise outages. You can discover all interdependent systems that need to migrate together, assess system configuration and capacity, and identify whether a running system is still serving users or is a candidate for decommissioning instead of migration. After the move is done, you can check on client load and identity to verify that test systems and customers are connecting. If your subnet planning and firewall definitions have issues, failed connections in Service Map maps will point you to the systems that need connectivity.

Business continuity

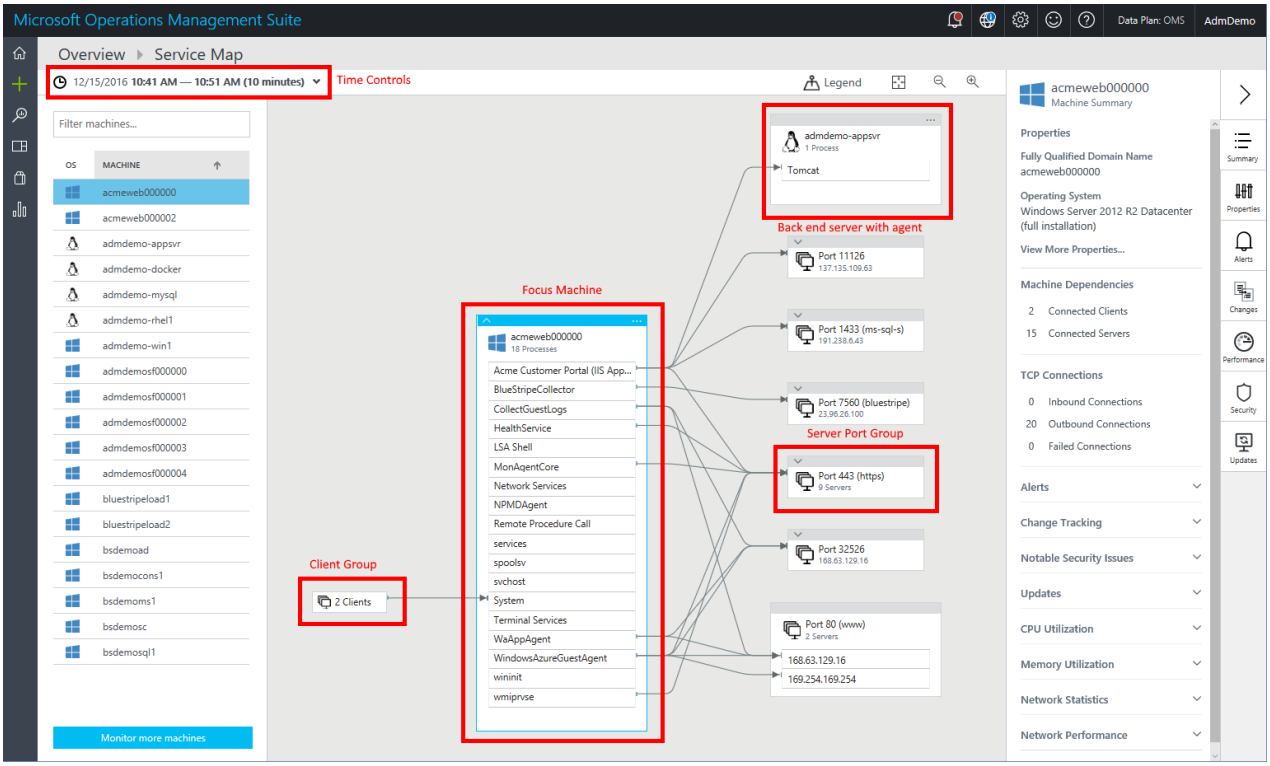
If you are using Azure Site Recovery and need help defining the recovery sequence for your application environment, Service Map can automatically show you how systems rely on each other to ensure that your recovery plan is reliable. By choosing a critical server and viewing its clients, you can identify the front-end systems that should be recovered only after that critical server is restored and available. Conversely, by looking at a critical server's back-end dependencies, you can identify those systems that must be recovered before your focus system is restored.

Patch management

Service Map enhances your use of OMS System Update Assessment by showing you which other teams and servers depend on your service, so you can notify them in advance before you take your systems down for patching. Service Map also enhances patch management in OMS by showing you whether your services are available and properly connected after they are patched and restarted.

Mapping overview

Service Map agents gather information about all TCP-connected processes on the server where they're installed, as well as details about the inbound and outbound connections for each process. Using the Machine List on the left side of the Service Map solution, machines with Service Map agents can be selected to visualize their dependencies over a selected time range. Machine dependency maps focus on a specific machine, and show all the machines that are direct TCP clients or servers of that machine.



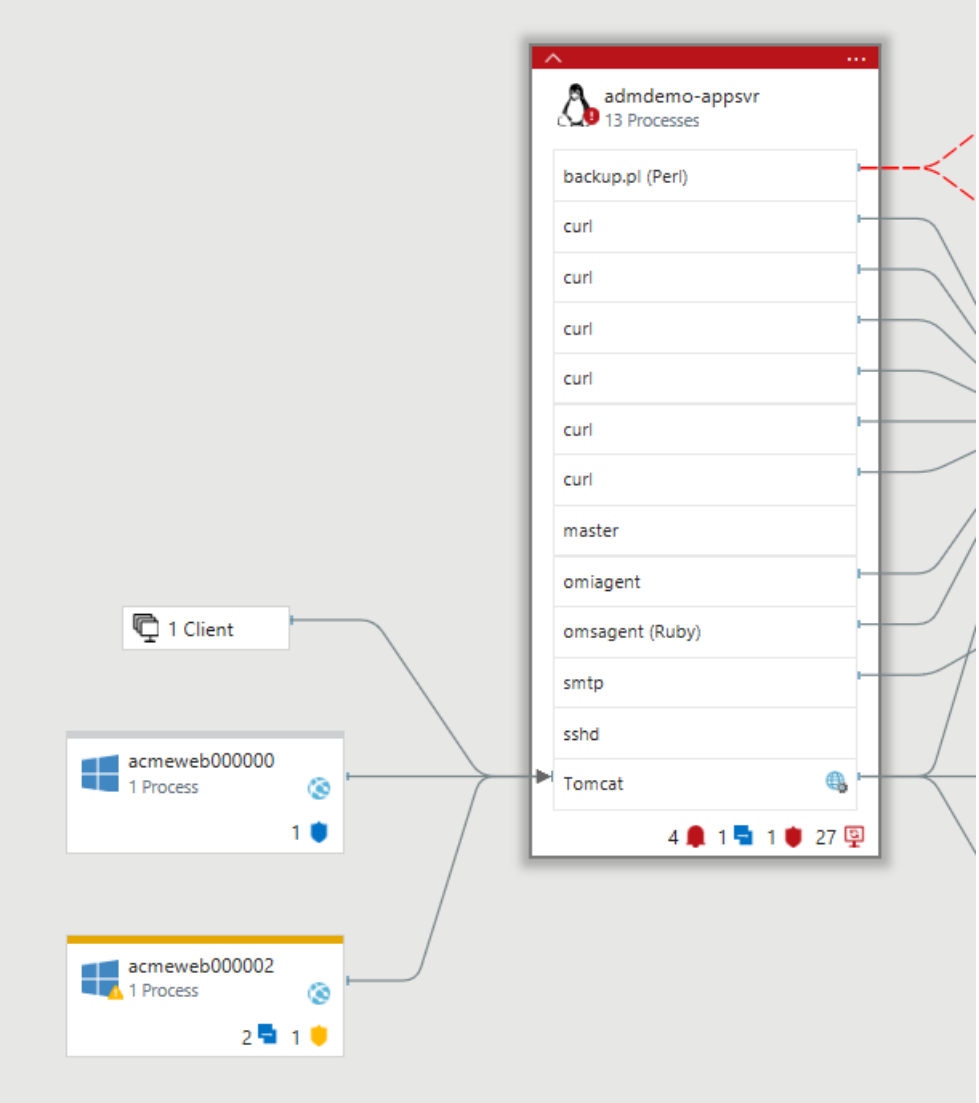
Machines can be expanded in the map to show the running processes with active network connections during the selected time range. When a remote machine with a Service Map agent is expanded to show process details, only those processes communicating with the focus machine are shown. The count of agentless front-end machines connecting into the focus machine is indicated on the left side of the processes they connect to. If the focus machine is making a connection to a back-end machine without an agent, that back-end server is included in a Server Port Group, along with other connections to the same port number.

By default, Service Map maps show the last 10 minutes of dependency information. Using the time controls in the upper left, maps can be queried for historical time ranges, up to one-hour wide, to show how dependencies looked in the past, e.g. during an incident or before a change occurred. Service Map data is stored for 30 days in paid workspaces, and for 7 days in free workspaces.

Status badges and border coloring

At the bottom of each server in the map can be a list of status badges conveying status information about the server. The badges indicate that there is some relevant information for the server from one of the OMS solution integrations. Clicking on a badge will take you directly to the details of the status in in the right panel. The currently availably status badges include Alerts, Changes, Security, and Updates.

Based on the severity of the status badges, machine node borders can be colored red (Critical), yellow (Warning), or blue (Informational). The color represents the most severe status of any of the status badges. A grey border indicates a node with no current status indicators.

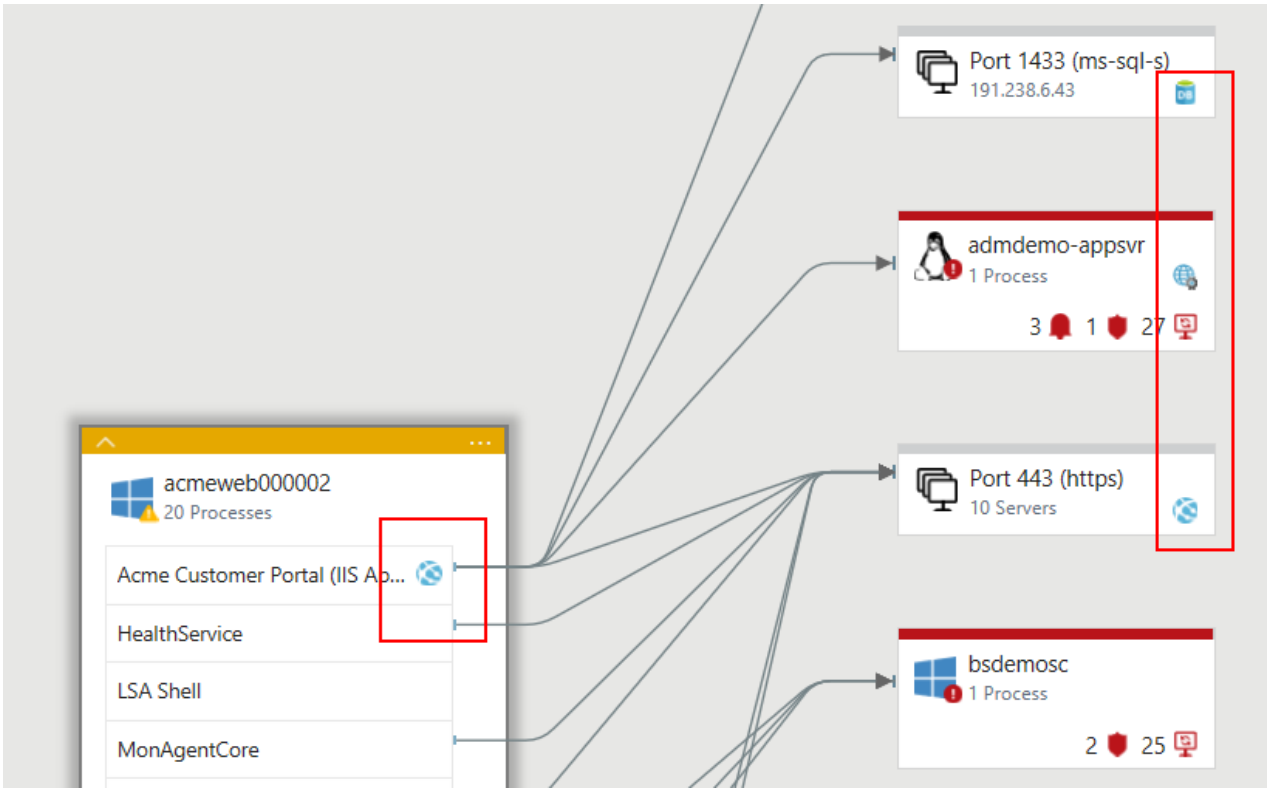


Role icons

Certain processes serve particular roles on machines: web servers, application servers, database, etc. Service Map will annotate process and machine boxes with role icons to help identify at a glance the role a process or server plays.

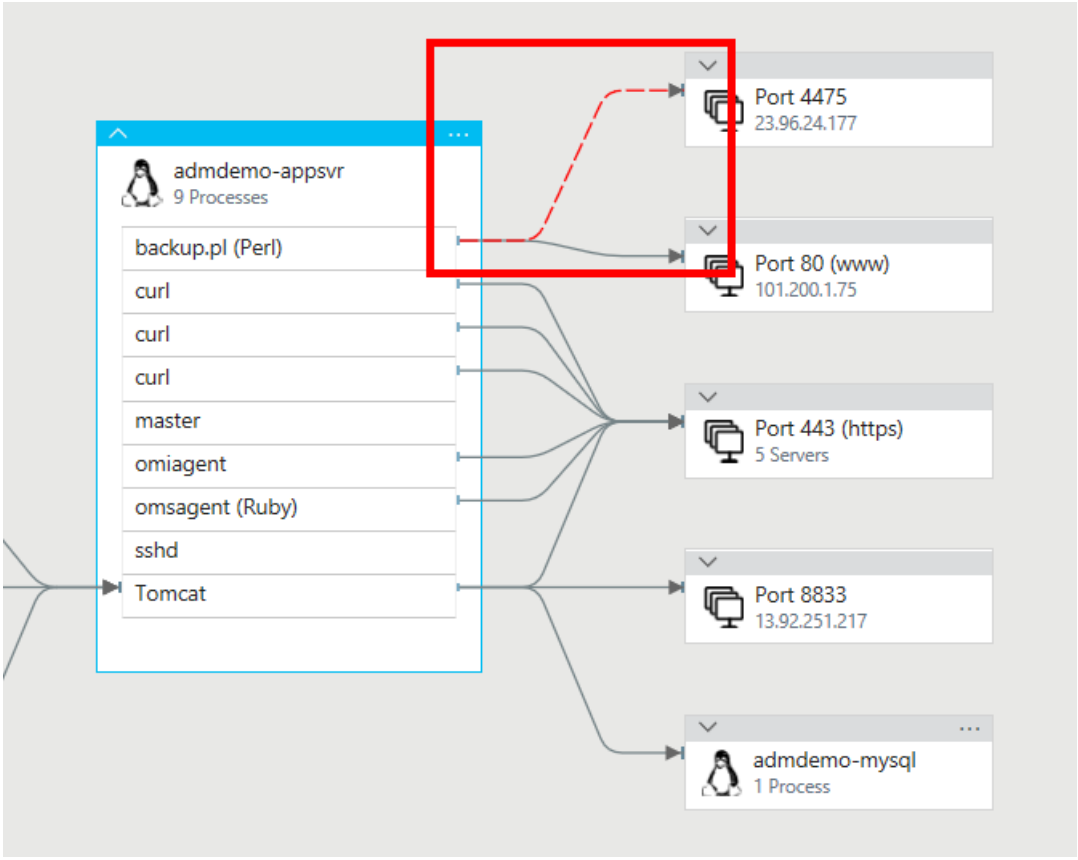
ROLE ICON	DESCRIPTION
	Web Server
	Application Server
	Database Server
	LDAP Server

ROLE ICON	DESCRIPTION
	SMB Server



Failed connections

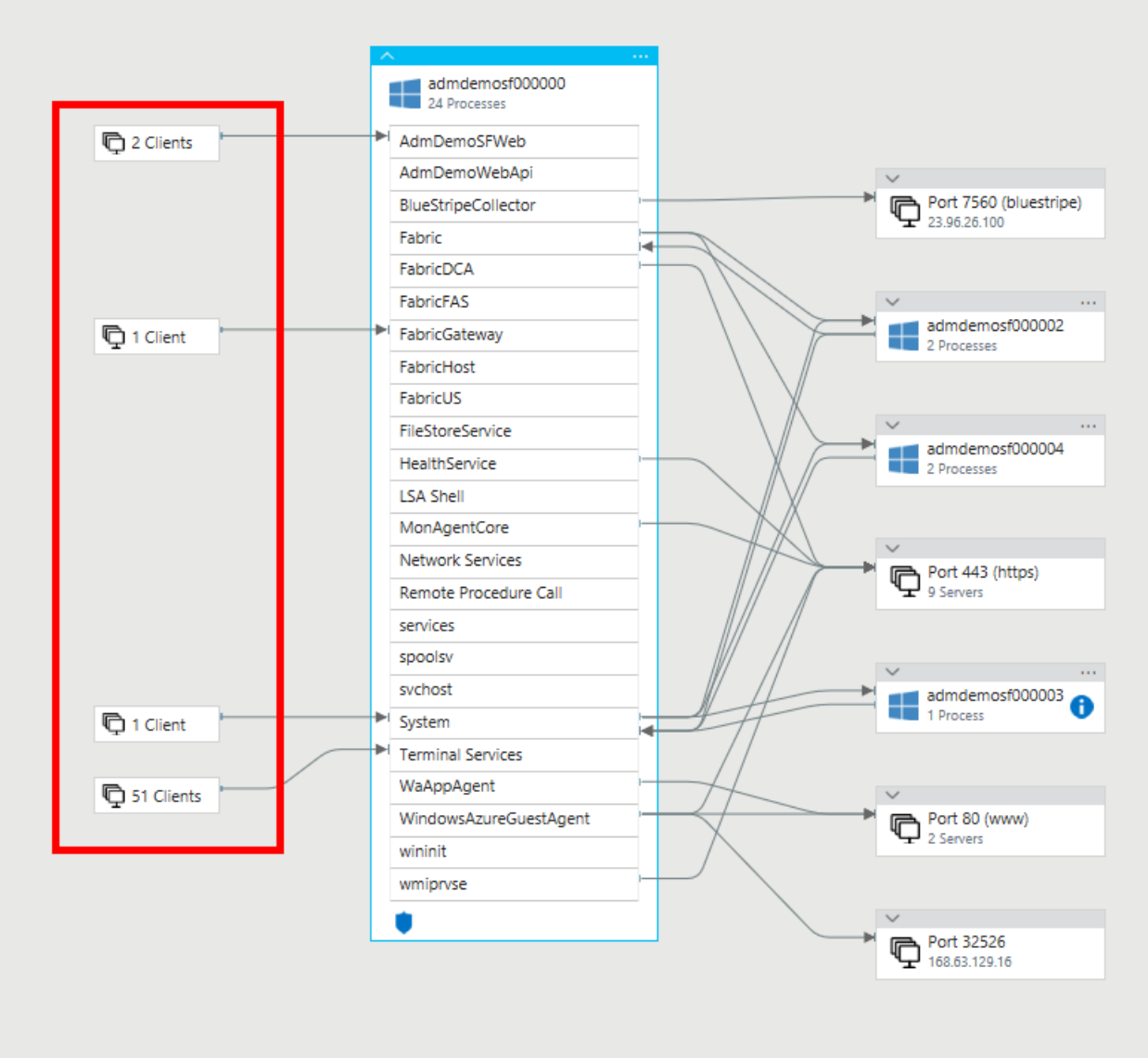
Failed Connections are shown in Service Map maps for processes and computers, with a dashed red line showing if a client system is failing to reach a process or port. Failed connections are reported from any system with a deployed Service Map agent if that system is the one attempting the failed connection. Service Map measures this by observing TCP sockets that fail to establish a connection. This could be due to a firewall, a misconfiguration in the client or server, or a remote service being unavailable.



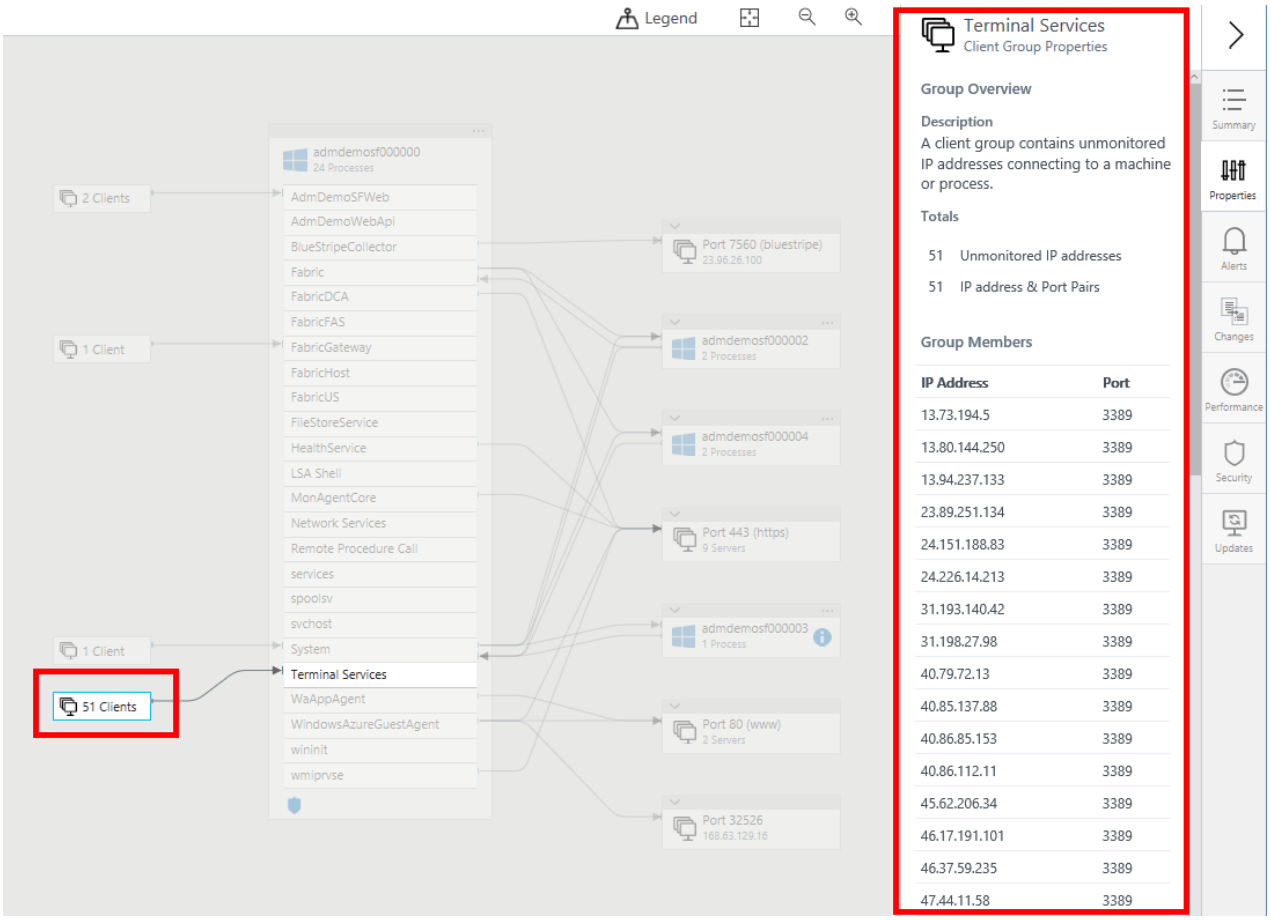
Understanding failed connections can help with troubleshooting, migration validation, security analysis, and overall architectural understanding. Sometimes failed connections are harmless, but they often point directly to a problem, such as a failover environment suddenly becoming unreachable, ...or two application tiers not being able to talk after a cloud migration.

Client Groups

Client Groups are boxes on the map that represent client machines that do not have Dependency Agents. A single Client Group represents the clients for an individual process.

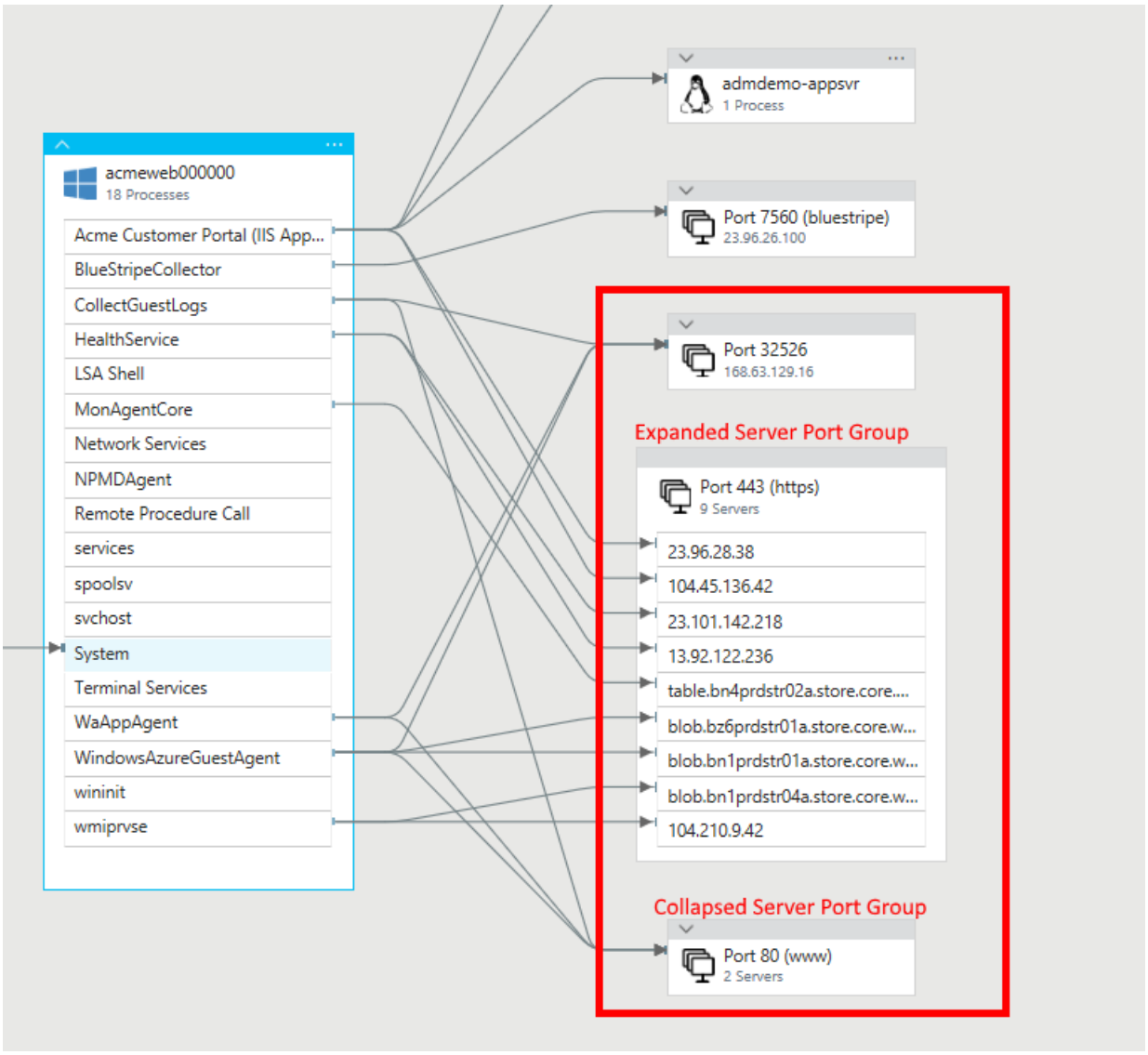


To see the IP addresses of the servers in a Client Group, select the group. The contents of the group will be listed in the Properties Panel.



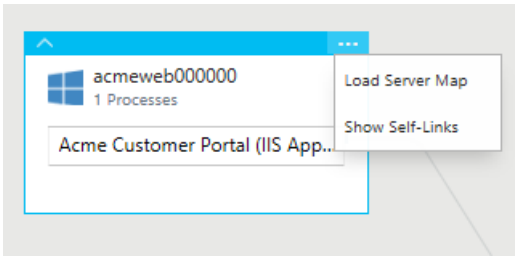
Server Port Groups

Server Port Groups are boxes that represent server ports on servers that do not have Dependency Agents. The box will list the server port along with a count of the number of servers with connections to that port. Expand the box to see the individual servers and connections. If there is only one server in the box, the name or IP address will be listed.



Context menu

Clicking on the three dots in the top right of any server will expose the context menu for that server.



Load Server Map

Load Server Map will navigate to a new map with the selected server as the new Focus Machine.

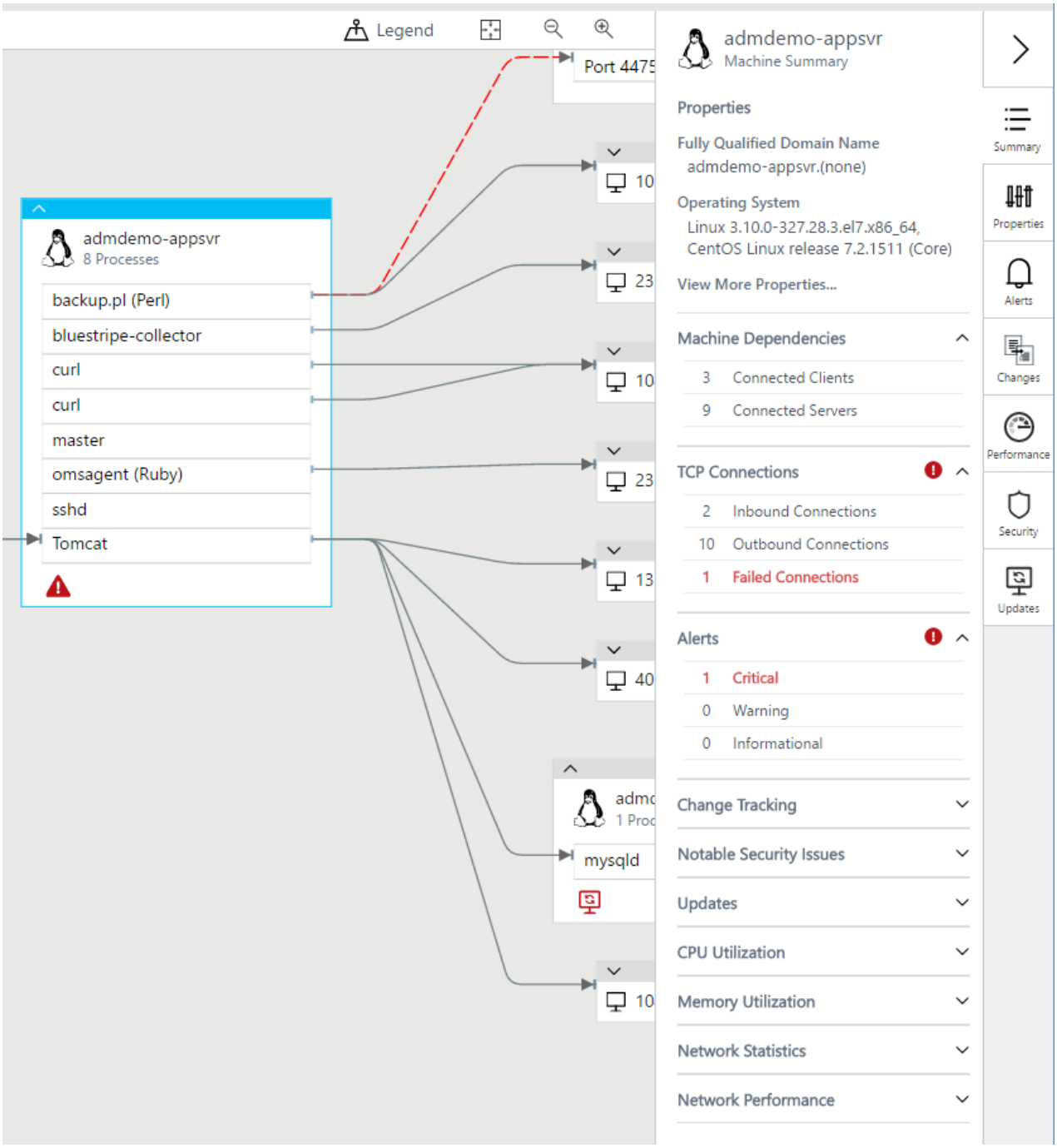
Show/Hide Self Links

Show Self Links will redraw the server node including any self links, which are TCP connections that start and end on processes within the server. If self links are shown, the menu will change to Hide Self Links, allowing users to toggle the drawing of self links.

Computer summary

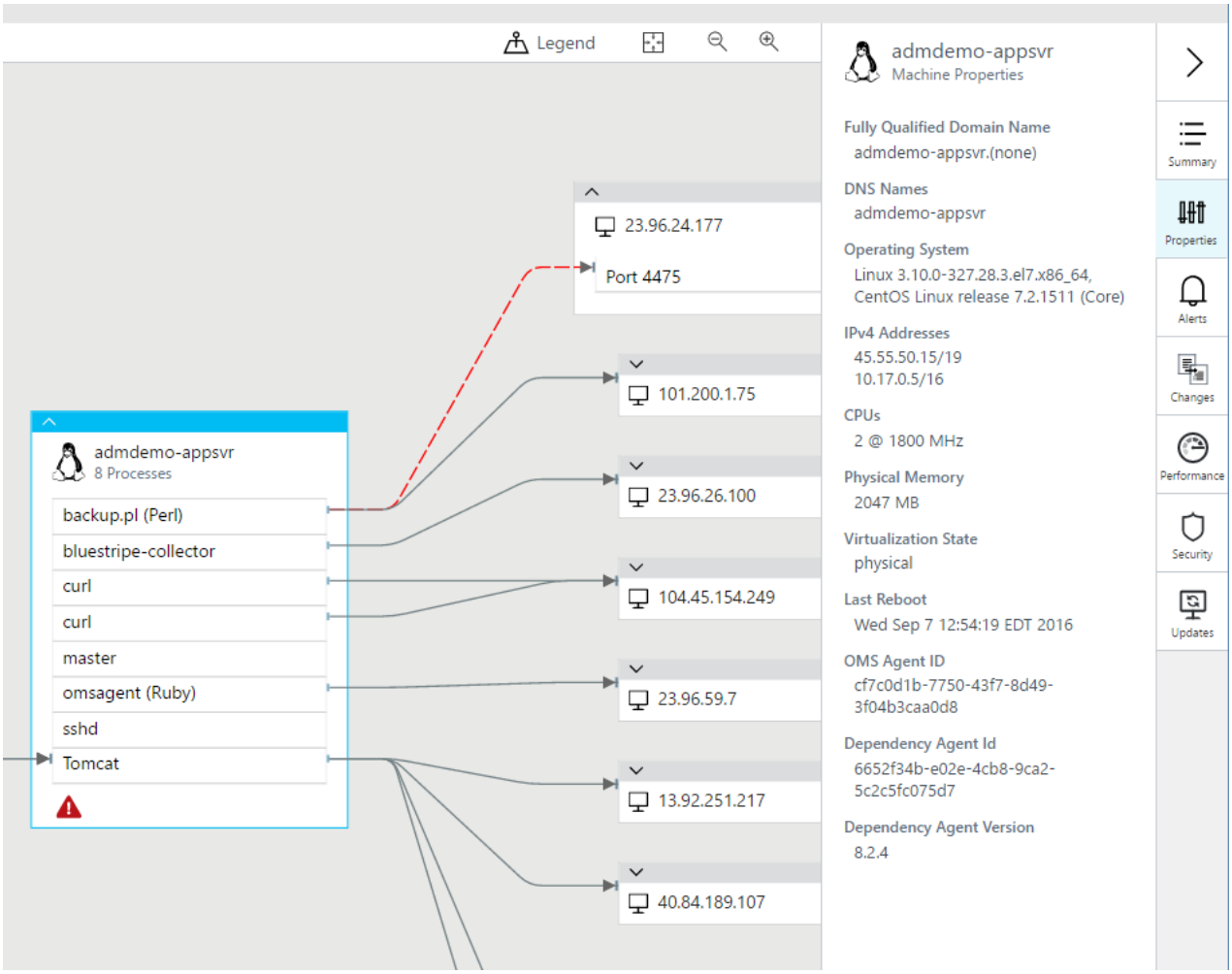
The Machine Summary panel includes an overview of a server's Operating System and dependency counts along with a variety of data from other OMS solutions, including Performance Metrics, Change Tracking, Security,

Updates, etc.

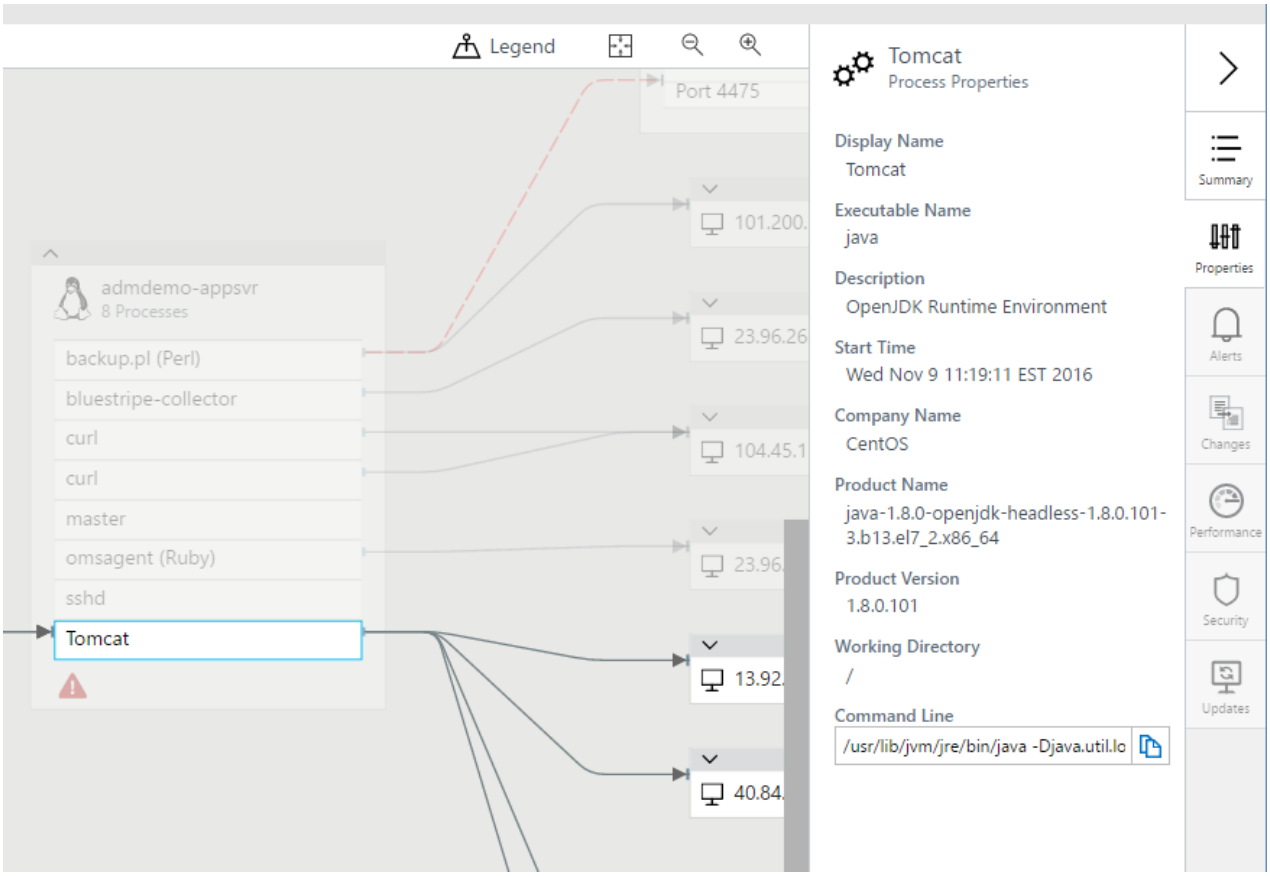


Computer and process properties

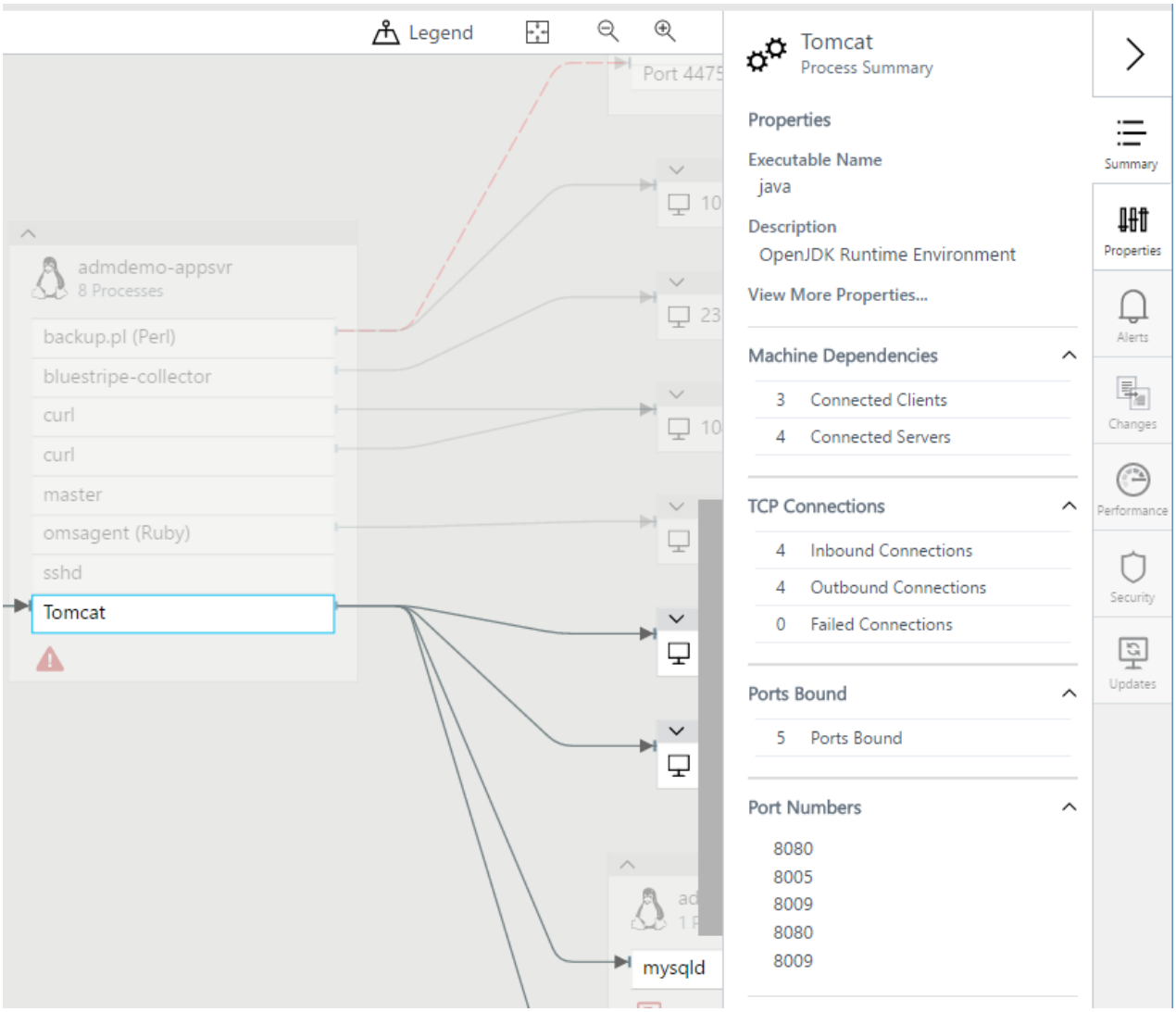
When navigating a Service Map map, you can select machines and processes to gain additional context about their properties. Machines provide information about DNS name, IPv4 addresses, CPU and Memory capacity, VM Type, Operating System version, Last Reboot time, and the IDs of their OMS and Service Map agents.



Process details are gathered from Operating System metadata about running processes, including process name, process description, user name and domain (on Windows), company name, product name, product version, working directory, command line, and process start time.

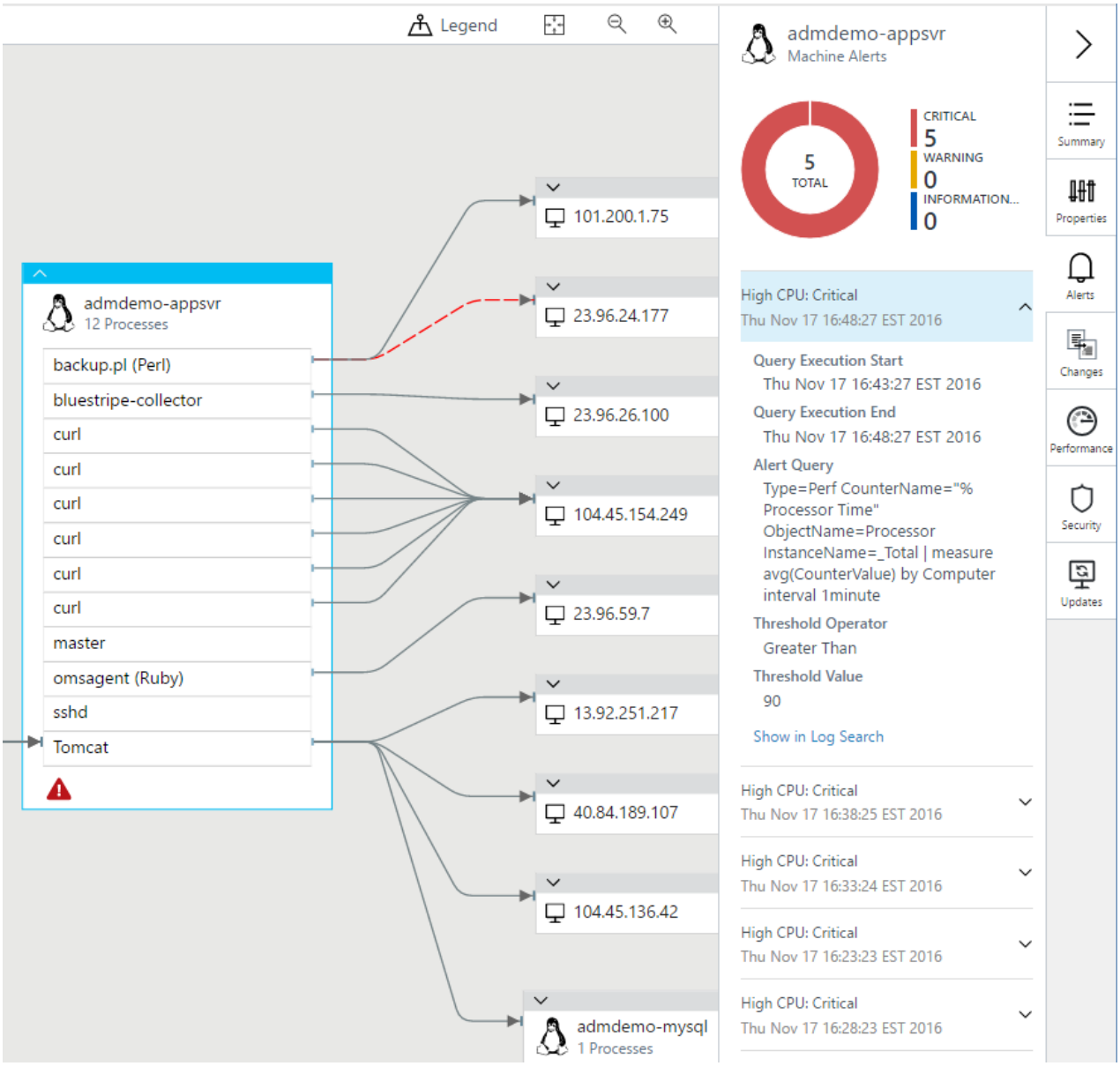


The Process Summary panel provides additional information about that process's connectivity, including its bound ports, inbound and outbound connections, and failed connections.



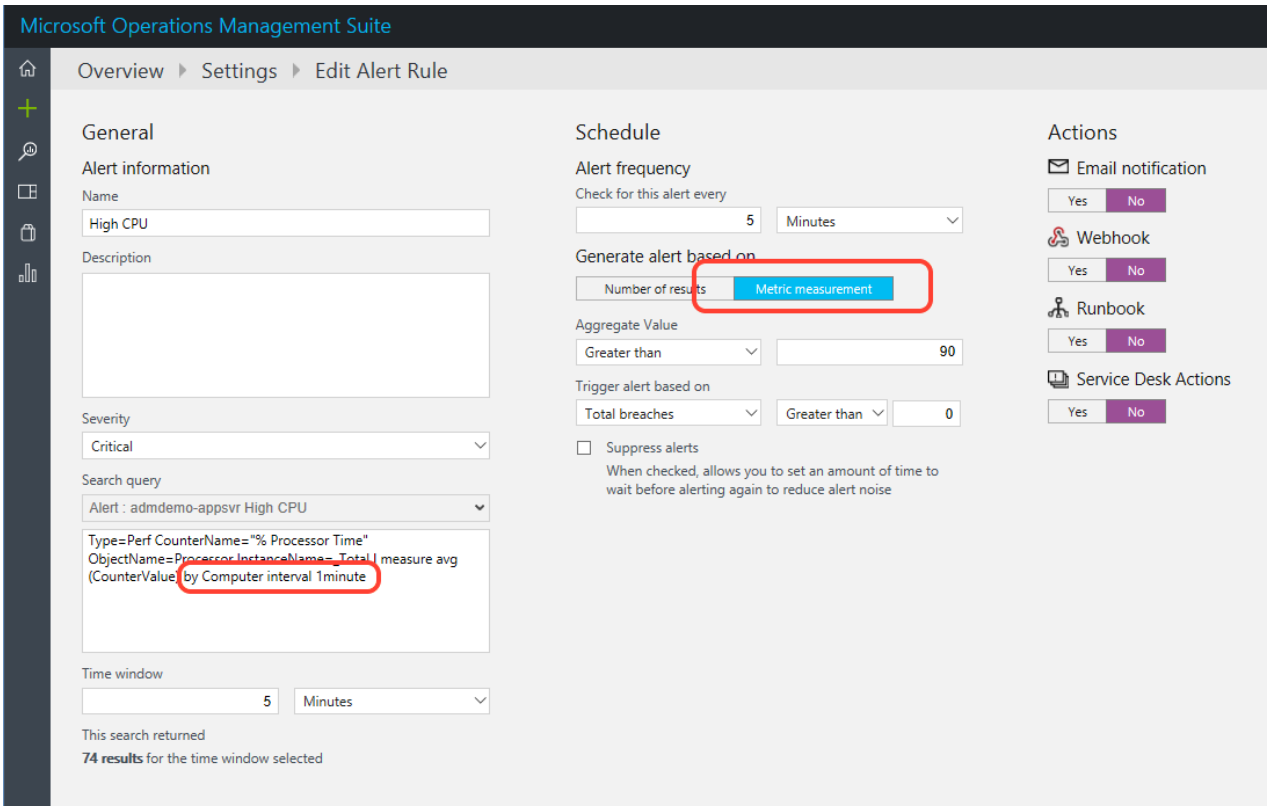
OMS Alerts integration

Service Map integrates with OMS Alerts to show fired alerts for the selected server in the selected time range. The server will show an icon if there are current alerts and the Machine Alerts Panel will list the alerts



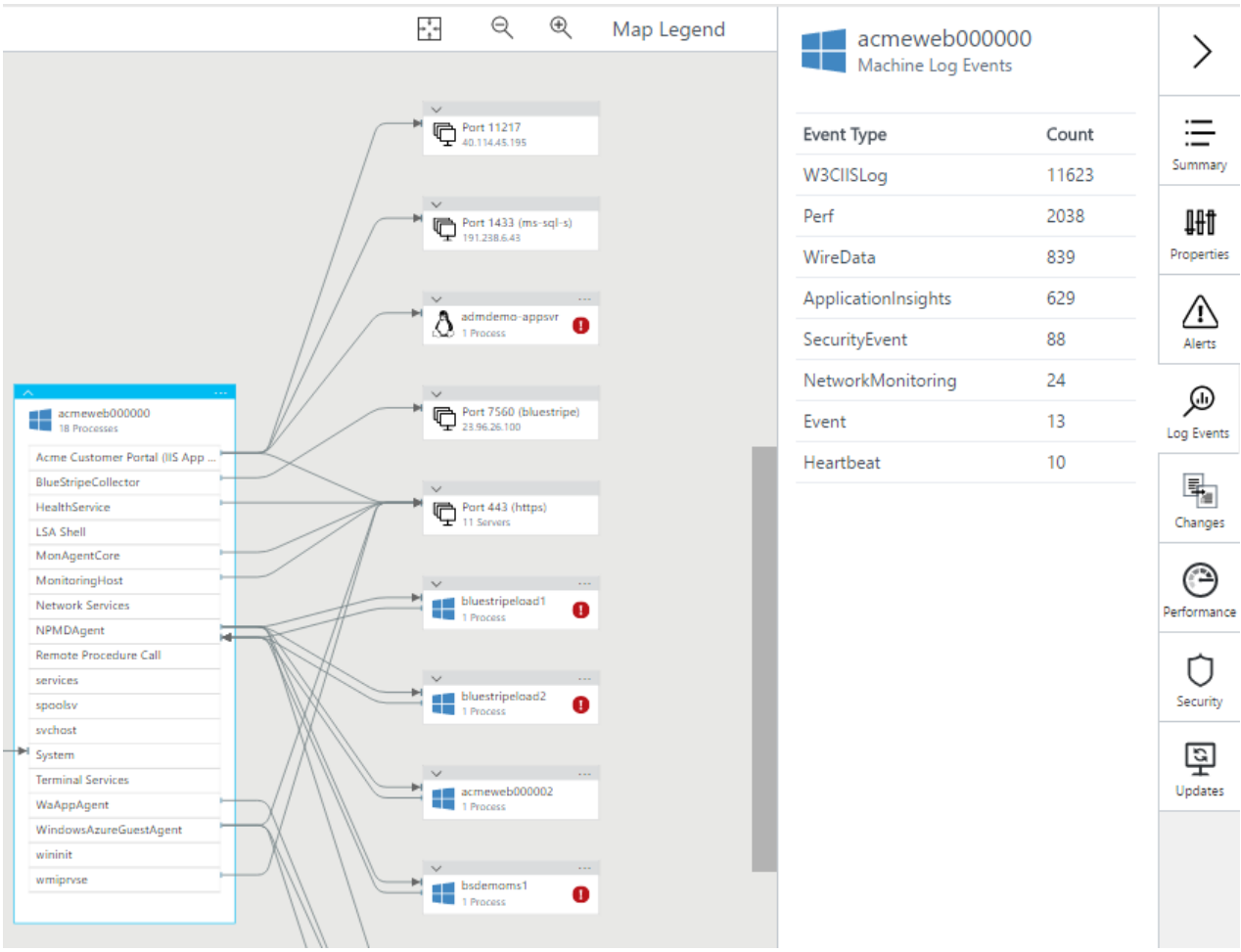
Note that for Service Map to be able to display relevant alerts, the alert rule must be created so that it fires for a specific computer. To create proper alerts:

- Include a clause to group by computer: "by Computer interval 1minute"
- Choose to alert based on Metric measurement



OMS Log Events integration

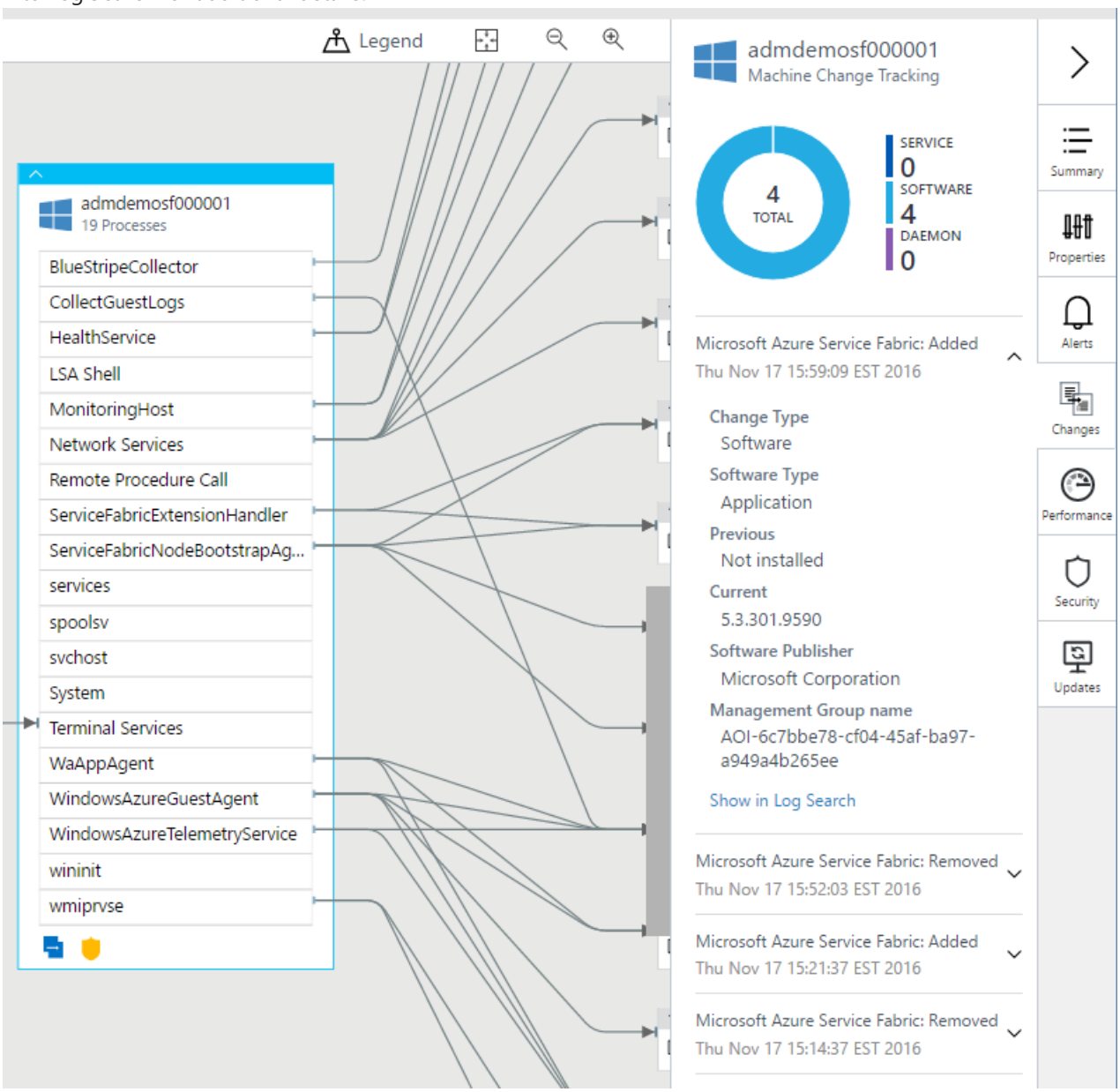
Service Map integrates with Log Search to show a count of all available log events for the selected server during the selected time range. You can click on any row in the list of event counts to jump to Log Search and see the individual log events.



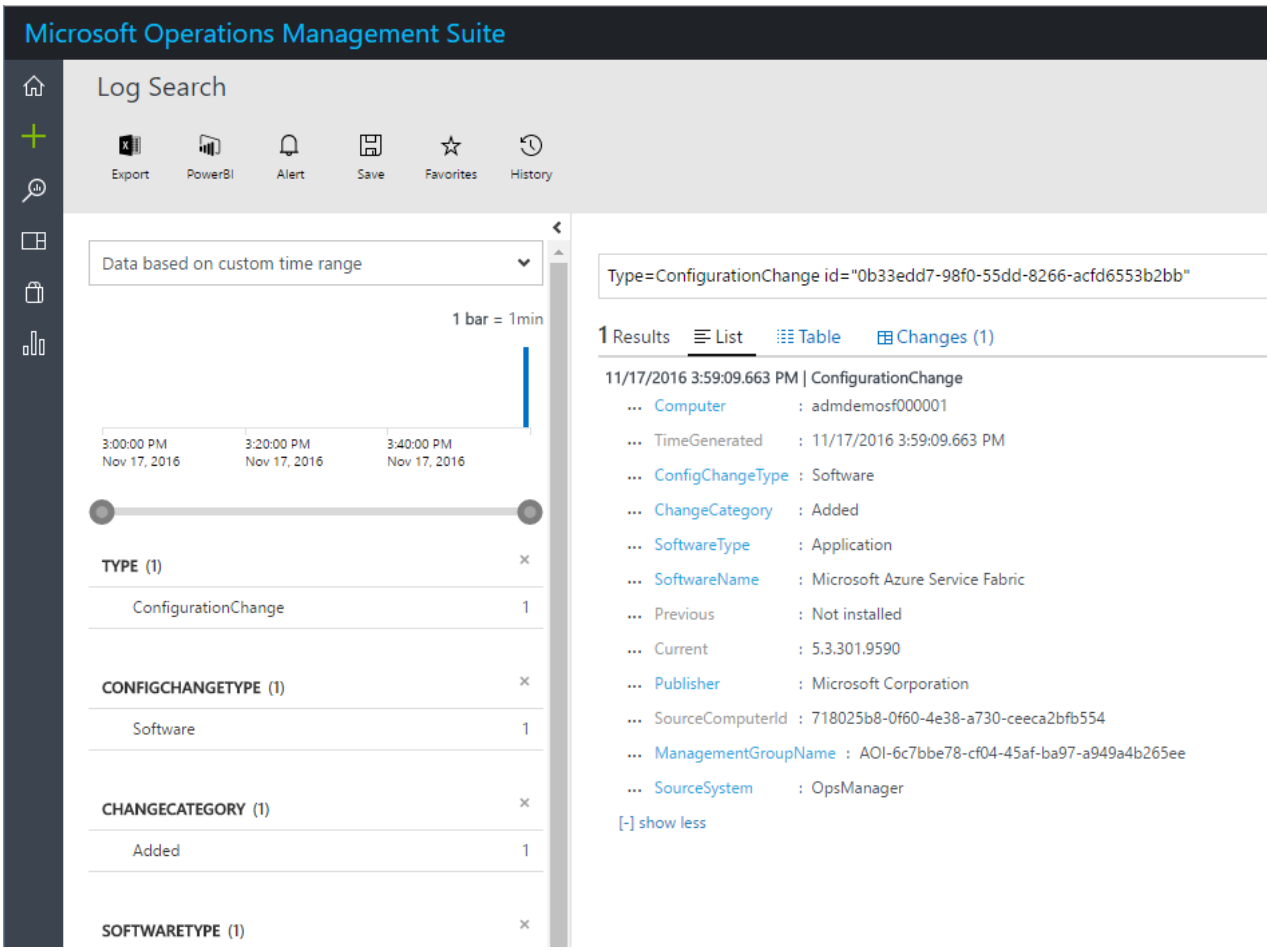
OMS Change Tracking integration

Service Map's integration with Change Tracking is automatic when both solutions are enabled and configured in your OMS workspace.

The Machine Change Tracking Panel shows a list of all changes, with the most recent first, along with a link to drill into Log Search for additional details.

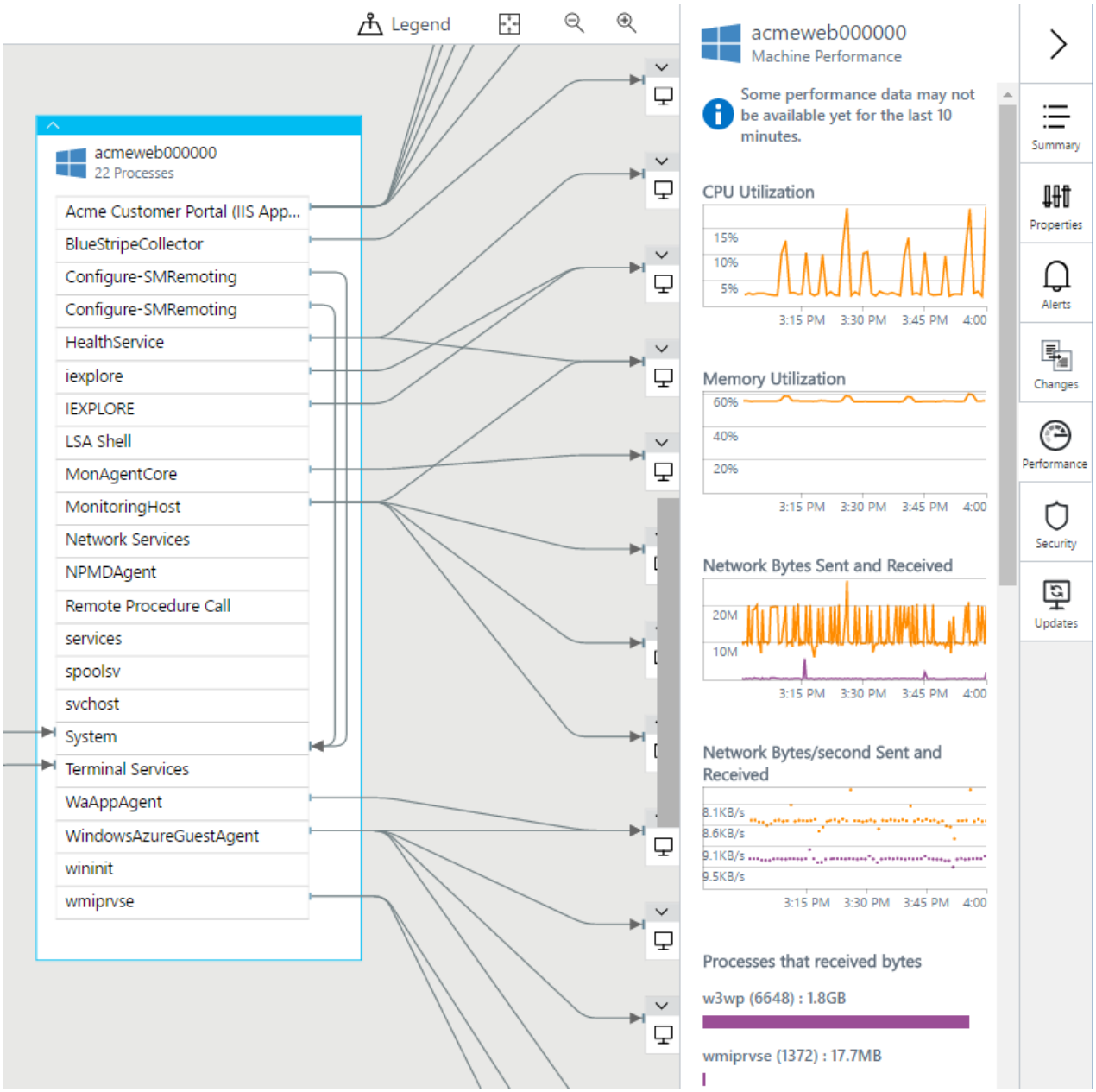


Following is a drill-down view of Configuration Change event after selecting **Show in Log Analytics**.



OMS Performance integration

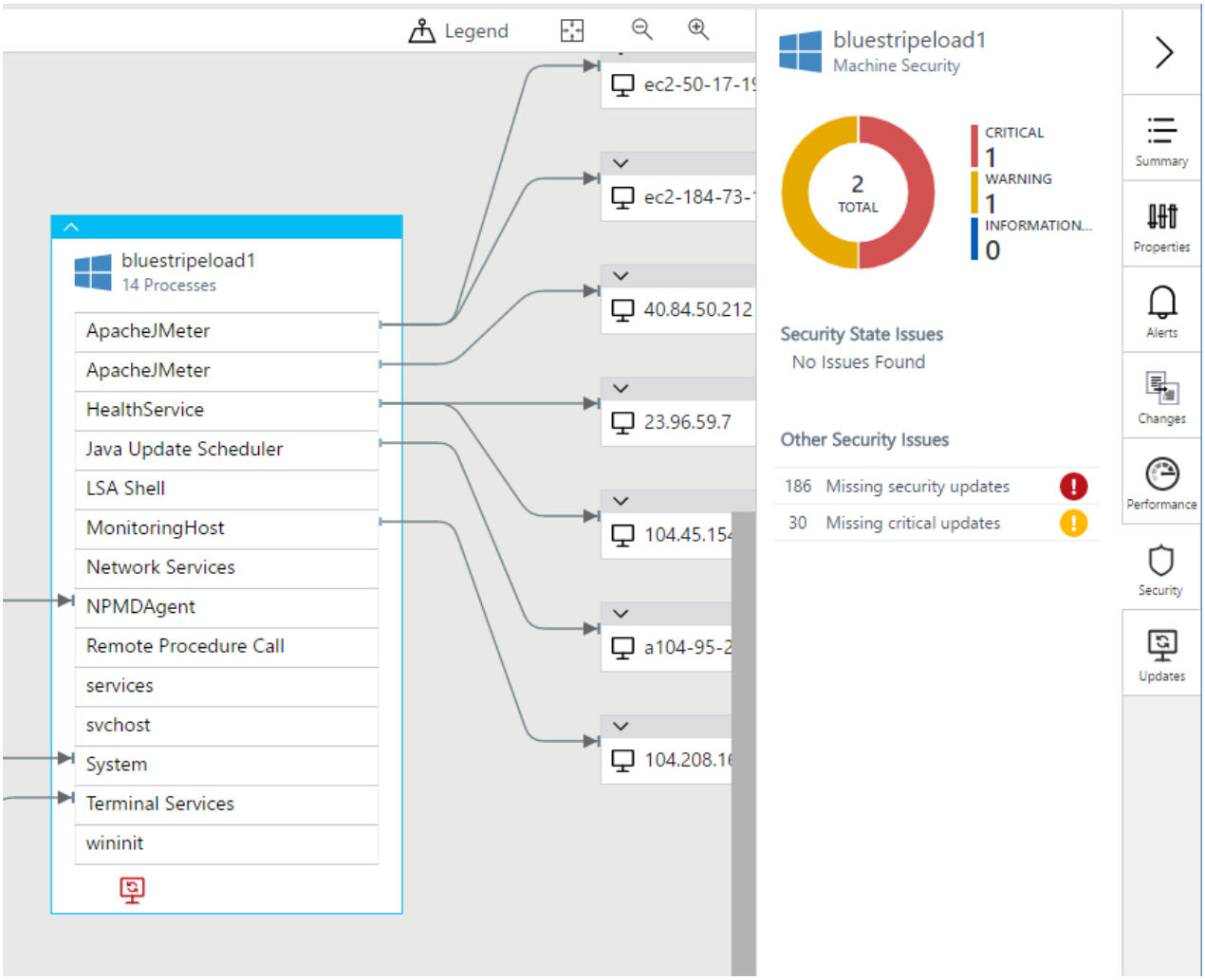
The Machine Performance Panel shows standard performance metrics for the selected server. The metrics include CPU Utilization, Memory Utilization, Network Bytes Sent and Received, and a list of the top processes by Network Bytes sent and received. Note that to get the network performance data, you must also have enabled the Wire Data 2.0 solution in OMS.



OMS Security integration

Service Map's integration with Security and Audit is automatic when both solutions are enabled and configured in your OMS workspace.

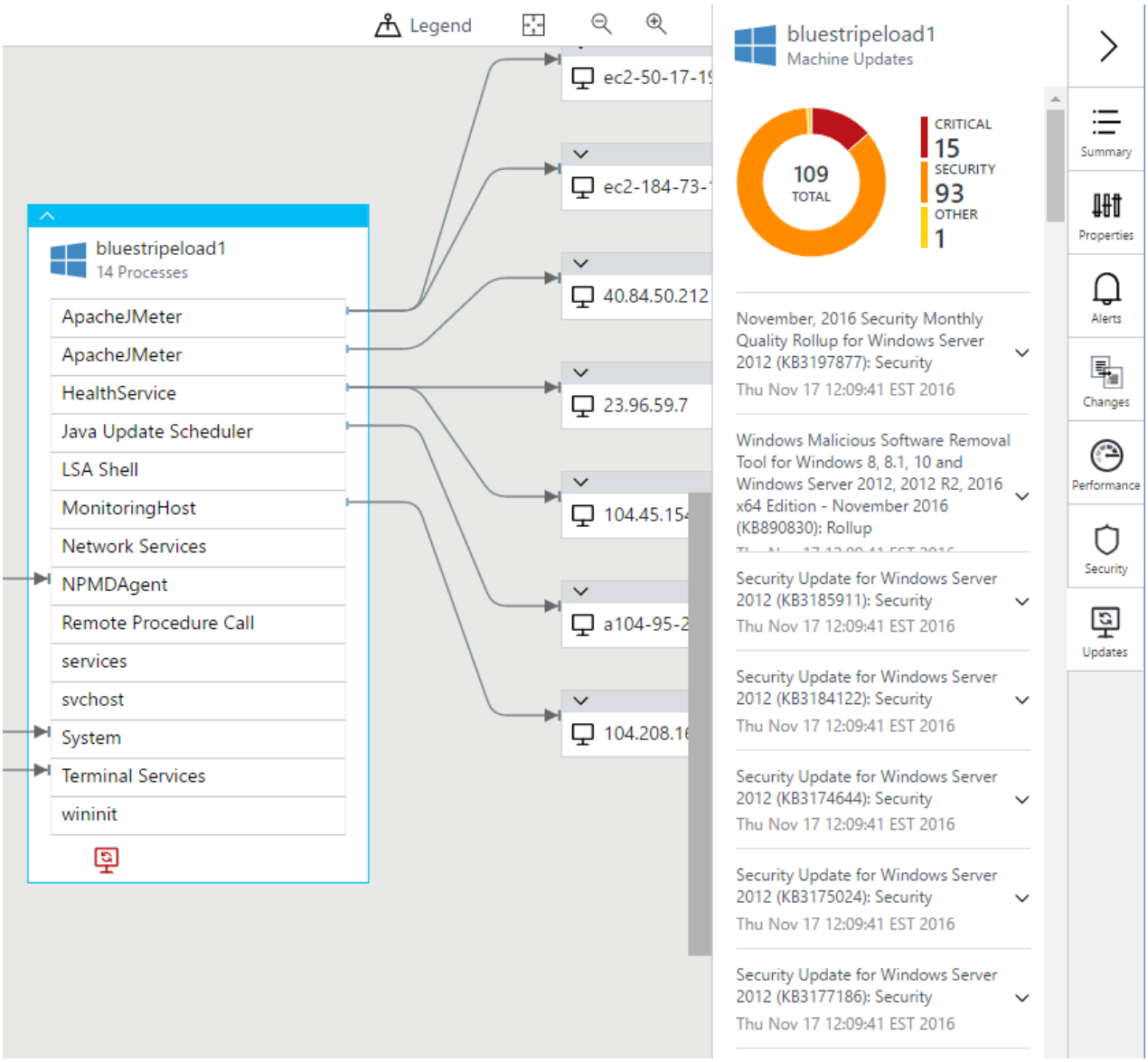
The Machine Security Panel shows data from the OMS Security and Audit solution for the selected server. The panel will list a summary of any outstanding security issues for the server during the selected time range. Clicking on any of the security issues will drill down into a Log Search for details about the security issues.



OMS Updates integration

Service Map's integration with Update Management is automatic when both solutions are enabled and configured in your OMS workspace.

The Machine Updates Panel shows data from the OMS Update Management solution for the selected server. The panel will list a summary of any missing updates for the server during the selected time range.



Log Analytics records

Service Map's computer and process inventory data is available for search in Log Analytics. This can be applied to scenarios including migration planning, capacity analysis, discovery, and ad hoc performance troubleshooting.

One record is generated per hour for each unique computer and process in addition to records generated when a process or computer starts or is on-boarded to Service Map. These records have the properties in the following tables. The fields and values in the ServiceMapComputer_CL events map to fields of the Machine resource in the ServiceMap ARM API. The fields and values in the ServiceMapProcess_CL events map to the fields of the Process resource in the ServiceMap ARM API. The ResourceName_s field matches the name field in the corresponding ARM resource. Note - as Service Map features grow, these fields are subject to change.

There are internally generated properties you can use to identify unique processes and computers:

- Computer - Use ResourceId or ResourceName_s to uniquely identify a computer within an OMS Workspace.
- Process - Use ResourceId to uniquely identify a process within an OMS Workspace. ResourceName_s is unique within the context of the machine on which the process is running (MachineResourceName_s)

Since multiple records can exist for a given process and computer in a given time range, queries can return more than one record for the same computer or process. To include only the most recent record add "| dedup ResourceId" to the query.

ServiceMapComputer_CL records

Records with a type of **ServiceMapComputer_CL** have inventory data for servers with Service Map agents. These

records have the properties in the following table:

PROPERTY	DESCRIPTION
Type	*ServiceMapComputer_CL*
SourceSystem	*OpsManager*
ResourceId	unique identifier for machine within the workspace
ResourceName_s	unique identifier for machine within workspace
ComputerName_s	computer FQDN
Ipv4Addresses_s	a list of the server's IPv4 addresses
Ipv6Addresses_s	a list of the server's IPv6 addresses
DnsNames_s	array of DNS names
OperatingSystemFamily_s	windows or linux
OperatingSystemFullName_s	operating system full name
Bitness_s	bitness of machine (32bit) or (64bit)
PhysicalMemory_d	physical memory in MB
Cpus_d	number of cpus
CpuSpeed_d	cpu speed in MHz
VirtualizationState_s	"unknown", "physical", "virtual", "hypervisor"
VirtualMachineType_s	"hyperv", "vmware", etc.
VirtualMachineNativeMachineId_g	VM ID as assigned by its hypervisor
VirtualMachineName_s	VM name
BootTime_t	boot time

ServiceMapProcess_CL Type records

Records with a type of **ServiceMapProcess_CL** have inventory data for TCP-connected processes on servers with Service Map agents. These records have the properties in the following table:

PROPERTY	DESCRIPTION
Type	*ServiceMapProcess_CL*
SourceSystem	*OpsManager*

PROPERTY	DESCRIPTION
ResourceId	unique identifier for process within the workspace
ResourceName_s	unique identifier for process within machine on which it is running
MachineResourceName_s	machine resource name
ExecutableName_s	process executable name
StartTime_t	process pool start time
FirstPid_d	first pid in process pool
Description_s	process description
CompanyName_s	company name
InternalName_s	internal name
ProductName_s	product name
ProductVersion_s	product version
FileVersion_s	file version
CommandLine_s	command line
ExecutablePath _s	path to executable file
WorkingDirectory_s	working directory
UserName	account under which the process is executing
UserDomain	domain under which the process is executing

Sample log searches

List all known machines

Type=ServiceMapComputer_CL | dedup ResourceId

List the physical memory capacity of all managed computers.

Type=ServiceMapComputer_CL | select PhysicalMemory_d, ComputerName_s | Dedup ResourceId

List computer name, DNS, IP, and OS.

Type=ServiceMapComputer_CL | select ComputerName_s, OperatingSystemFullName_s, DnsNames_s, IPv4Addresses_s | dedup ResourceId

Find all processes with "sql" in the command line

Type=ServiceMapProcess_CL CommandLine_s = *sql* | dedup ResourceId

Find a machine (most recent record) by resource name

Type=ServiceMapComputer_CL "m-4b9c93f9-bc37-46df-b43c-899ba829e07b" | dedup ResourceId

Find a machine (most recent record) by ip address

Type=ServiceMapComputer_CL "10.229.243.232" | dedup ResourceId

List all known processes on a given machine

Type=ServiceMapProcess_CL MachineResourceName_s="m-4b9c93f9-bc37-46df-b43c-899ba829e07b" | dedup ResourceId

List all computers running SQL

Type=ServiceMapComputer_CL ResourceName_s IN {Type=ServiceMapProcess_CL *sql* | Distinct MachineResourceName_s} | dedup ResourceId | Distinct ComputerName_s

List of all unique product versions of curl in my datacenter

Type=ServiceMapProcess_CL ExecutableName_s=curl | Distinct ProductVersion_s

Create a Computer Group of all computers running CentOS

Type=ServiceMapComputer_CL OperatingSystemFullName_s = *CentOS* | Distinct ComputerName_s

REST API

All of the server, process, and dependency data in Service Map is available via the Service Map REST API.

Diagnostic and usage data

Microsoft automatically collects usage and performance data through your use of the Service Map service. Microsoft uses this Data to provide and improve the quality, security, and integrity of the Service Map service. Data includes information about the configuration of your software like operating system and version and also includes IP address, DNS name, and Workstation name in order to provide accurate and efficient troubleshooting capabilities. We do not collect names, addresses, or other contact information.

For more information on data collection and usage, please see the Microsoft Online Services Privacy Statement.

Next steps

- Learn more about log searches in Log Analytics to retrieve data collected by Service Map.

Troubleshooting

- See the Troubleshooting section of the Configuring Service Map document.

Feedback

Do you have any feedback for us about Service Map or this documentation? Please visit our User Voice page, where you can suggest features or vote up existing suggestions.

Configuring Service Map solution in Operations Management Suite (OMS)

4/19/2017 • 12 min to read • Edit Online

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. It allows you to view your servers as you think of them – as interconnected systems that deliver critical services. Service Map shows connections between servers, processes, and ports across any TCP-connected architecture with no configuration required other than installation of an agent.

This article describes the details of configuring Service Map and onboarding agents. For information on using Service Map, see Using Service Map solution in Operations Management Suite (OMS)

Dependency Agent downloads

FILE	OS	VERSION	SHA-256
InstallDependencyAgent-Windows.exe	Windows	9.0.5	73B3F6A2A76A08D58F72A550947FF839B588591C48E6EDDD6DDF73AA3FD82B43
InstallDependencyAgent-Linux64.bin	Linux	9.0.5	A1BAD0B36EBF79F2B69113A07FCF48C68D90BD169C722689F9C83C69FC032371

Connected sources

Service Map gets its data from the Microsoft Dependency Agent. The Dependency Agent is dependent on the OMS Agent for its connections to OMS. This means that a server must have the OMS Agent installed and configured first, and then the Dependency Agent can be installed. The following table describes the connected sources that are supported by the Service Map solution.

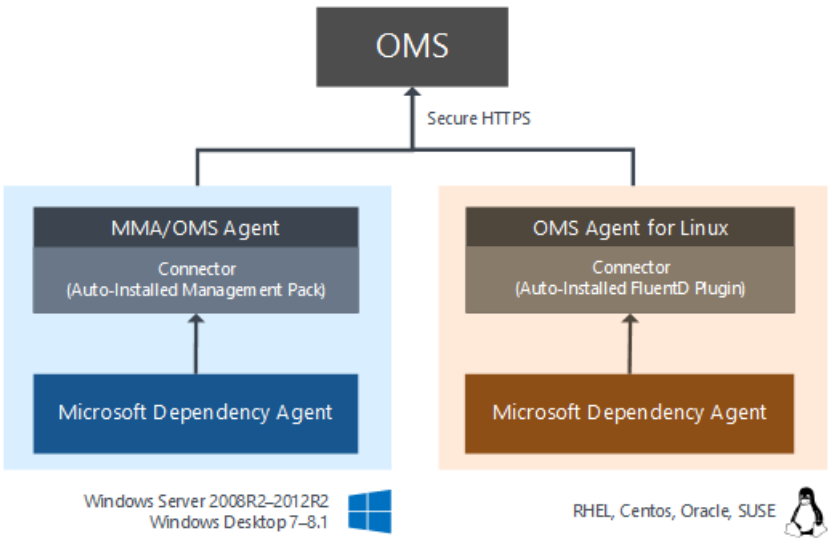
CONNECTED SOURCE	SUPPORTED	DESCRIPTION
Windows agents	Yes	Service Map analyzes and collects data from Windows agent computers. In addition to the OMS Agent, Windows agents require the Microsoft Dependency Agent. See the Supported Operating Systems for a complete list of operating system versions.
Linux agents	Yes	Service Map analyzes and collects data from Linux agent computers. In addition to the OMS Agent, Linux agents require the Microsoft Dependency Agent. See the Supported Operating Systems for a complete list of operating system versions.

CONNECTED SOURCE	SUPPORTED	DESCRIPTION
SCOM management group	Yes	Service Map analyzes and collects data from Windows and Linux agents in a connected System Center Operations Manager (SCOM) management group. A direct connection from the SCOM agent computer to OMS is required. Data is sent directly from forwarded from the management group to the OMS repository.
Azure storage account	No	Service Map collects data from agent computers, so there is no data from it to collect from Azure storage.

Service Map only supports 64-bit platforms.

On Windows, the Microsoft Monitoring Agent (MMA) is used by both SCOM and OMS to gather and send monitoring data. (This agent is called the SCOM Agent, OMS Agent, MMA, or Direct Agent, depending on context.) SCOM and OMS provide different out of the box versions of MMA, but these versions can each report to SCOM, to OMS, or to both. On Linux, the OMS Agent for Linux gathers and sends monitoring data to OMS. You can use Service Map on servers with OMS Direct Agents or on servers that are attached to OMS via SCOM Management Groups. In this documentation, we will refer to all agents – whether Linux or Windows, whether connected to a SCOM MG or directly to OMS – as the "OMS Agent", unless the specific deployment name of the agent is needed for context.

The Service Map agent does not transmit any data itself, and it does not require any changes to firewalls or ports. Service Map's data is always transmitted by the OMS Agent to OMS, either directly or via the OMS Gateway.



If you are a SCOM customer with a Management Group connected to OMS:

- If your SCOM agents can access the internet to connect to OMS, no additional configuration is required.
- If your SCOM agents cannot access OMS over the internet, you need to configure the OMS Gateway to work with SCOM.

If you are using the OMS Direct Agent, you need to configure the OMS Agent itself to connect to OMS or to your OMS Gateway. The OMS Gateway can be downloaded from https://www.microsoft.com/download/details.aspx?id=52666

Avoiding duplicate data

If you are a SCOM customer, you should not configure your SCOM agents to communicate directly to OMS, or data will be reported twice. In Service Map, this will result in computers appearing twice in the Machine List.

Configuration of OMS should happen in only one of the following locations:

- The SCOM Console Operations Management Suite panel for Managed Computers
- Azure Operational Insights configuration in the MMA properties

Using both configurations with the *same* workspace in each will cause duplication of data. Using both configurations with *different* workspaces can result in conflicting configuration (one with the Service Map solution enabled and the other without) that may prevent data from flowing to Service Map completely.

Even if the machine itself isn't specified in the SCOM Console's OMS configuration, if an Instance Group such as "Windows Server Instances Group" is active, it may still result in the machine receiving OMS configuration via SCOM.

Management packs

When Service Map is activated in an OMS workspace, a 300KB Management Pack is sent to all the Microsoft Monitoring Agents in that workspace. If you are using SCOM agents in a connected management group, the Service Map Management Pack will be deployed from SCOM. If the agents are directly connected, the MP will be delivered by OMS.

The MP is named Microsoft.IntelligencePacks.ApplicationDependencyMonitor. *It is written to *%Programfiles%\Microsoft Monitoring Agent\Agent\Health Service State\Management Packs*. The data source used by the management pack is *%Program files%\Microsoft Monitoring Agent\Agent\Health Service State\Resources<AutoGeneratedID>\Microsoft.EnterpriseManagement.Advisor.ApplicationDependencyMonitorDataSource.dll*.

Configuration

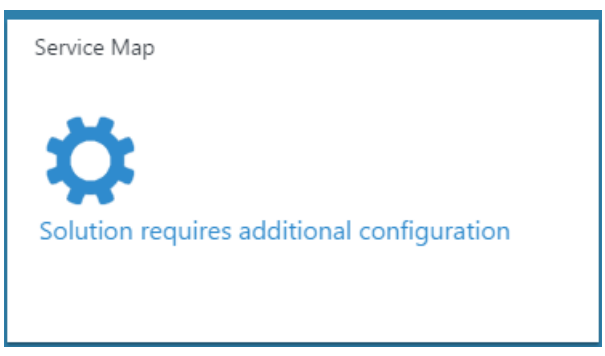
In addition to Windows and Linux computers have an agent installed and connected to OMS, the Dependency Agent installer must be downloaded from the Service Map solution and then installed as root or Admin on each managed server. Once the Service Map agent is installed on a server reporting to OMS, Service Map dependency maps will appear within 10 minutes.

Migrating from BlueStripe FactFinder

Service Map will deliver BlueStripe technology into OMS in phases. FactFinder is still supported for existing customers but is no longer available for individual purchase. This preview version of the Dependency Agent can only communicate with OMS. If you are a current FactFinder customer, please identify a set of test servers for Service Map that are not managed by FactFinder.

Download the Dependency Agent

In addition to the Microsoft Management Agent (MMA) and OMS Linux Agent, which provide the connection between the computer and OMS, all computers analyzed by Service Map must have the Dependency Agent installed. On Linux, the OMS Agent for Linux must be installed before the Dependency Agent.



To download the Dependency Agent, click **Configure Solution** in the **Service Map** tile to open the **Dependency Agent** blade. The Dependency Agent blade has links for the Windows and the Linux agents. See the following sections for details on installing the agent on different systems.

Install the Dependency Agent

Microsoft Windows

Administrator privileges are required to install or uninstall the agent.

The Dependency Agent is installed on Windows computers with InstallDependencyAgent-Windows.exe. If you run this executable without any options, then it will start a wizard that you can follow to install interactively.

Use the following steps to install the Dependency Agent on each Windows computer:

1. Ensure that the OMS Agent is installed using the instructions at Connect computers directly to OMS.
2. Download the Windows agent and run it with the following command:
   InstallDependencyAgent-Windows.exe
3. Follow the wizard to install the agent.
4. If the Dependency Agent fails to start, check the logs for detailed error information. On Windows agents, the log directory is *C:\Program Files\Microsoft Dependency Agent\logs*.

The Dependency Agent for Windows can be uninstalled by an Administrator through the Control Panel.

Linux

Root access is required to install or configure the agent.

The Dependency Agent is installed on Linux computers with InstallDependencyAgent-Linux64.bin, a shell script with a self-extracting binary. You can run the file with sh or add execute permissions to the file itself.

Use the following steps to install the Dependency Agent on each Linux computer:

1. Ensure that the OMS Agent is installed using the instructions at Collect and manage data from Linux computers. The OMS Agent needs to be installed before the Linux Dependency Agent.
2. Install the Linux Dependency agent as root using the following command:
   sh InstallDependencyAgent-Linux64.bin.
3. If the Dependency Agent fails to start, check the logs for detailed error information. On Linux agents, the log directory is */var/opt/microsoft/dependency-agent/log*.

Uninstalling the Dependency Agent on Linux

To completely uninstall the Dependency Agent from Linux, you must remove the agent itself and the Connector, which is installed automatically with the agent. You can uninstall both with the following single command:

```
rpm -e dependency-agent dependency-agent-connector
```

Installing from a command line

The previous section provides guidance on installing the Dependency Monitor agent using default options. The following sections provide guidance for installing the agent from a command line using custom options.

Windows

Use options from the following table to install from a command line. To see a list of the installation flags run the installer with the /? flag as follows.

```
InstallDependencyAgent-Windows.exe /?
```

FLAG	DESCRIPTION
/S	Perform a silent installation with no user prompts.

Files for the Windows Dependency Agent are placed in *C:\Program Files\Microsoft Dependency Agent* by default.

Linux

Use options from the following table to install. To see a list of the installation flags run the installation program with the -help flag as follows.

```
InstallDependencyAgent-Linux64.bin -help
```

FLAG	DESCRIPTION
-s	Perform a silent installation with no user prompts.
--check	Checks permissions and operating system but does not install the agent.

Files for the Dependency Agent are placed in the following directories:

FILES	LOCATION
Core files	/opt/microsoft/dependency-agent
Log files	/var/opt/microsoft/dependency-agent/log
Config files	/etc/opt/microsoft/dependency-agent/config
Service executables	/opt/microsoft/dependency-agent/bin/microsoft-dependency-agent /opt/microsoft/dependency-agent/bin/microsoft-dependency-agent-manager
Binary storage files	/var/opt/microsoft/dependency-agent/storage

Troubleshooting

If you run into any problems installing or running Service Map, this section can help you get up and running. If you still can't resolve your issue, please contact Microsoft Support.

Dependency Agent installation issues

Installer asks for a reboot

The Dependency Agent *generally* does not require a reboot upon installation or uninstallation. However, in certain rare cases, a Windows Server will require a reboot to continue with an installation. This happens when a dependency, usually the Microsoft VC++ Redistributables, requires a reboot due to a locked file.

Message "Unable to install Dependency Agent: Visual Studio Runtime libraries failed to install (code = [code_number])."

The Microsoft Dependency Agent is built upon the Microsoft Visual Studio Runtime Libraries. An issue was encountered while trying to install the libraries. The runtime library installers create logs in the %LOCALAPPDATA%\temp folder. The file will be dd_vcredist_arch_yyyymmddhhmmss.log, where arch will be "x86" or "amd64" and yyyymmddhhmmss will be the date and time (24 hour clock) when the log was created. The log will provide details about the issue blocking installation.

It might be useful to install the latest Runtime Libraries yourself first.

Below are some code_numbers and suggested resolutions.

CODE	DESCRIPTION	RESOLUTION
0x17	The library installer requires a Windows update that hasn't been installed.	Look in the most recent library installer log (see above). If a reference to "Windows8.1-KB2999226-x64.msu" is followed by a line "Error 0x80240017: Failed to execute MSU package.", then you do not have the necessary prerequisites installed to install KB2999226. Follow the instructions in the prerequisites section in https://support.microsoft.com/kb/2999226. Note that you may need to run Windows Update and reboot multiple times in order to install the necessary prerequisites. Run the Microsoft Dependency Agent installer again.

Post-Installation issues

Server doesn't show in Service Map

If your Dependency Agent installation succeeded, but you don't see your server in the Service Map solution:

1. Is the Dependency Agent installed successfully? You can validate this by checking to see if the service is installed and running.

   Windows: Look for the Service named "Microsoft Dependency Agent"
   Linux: Look for the running process "microsoft-dependency-agent"

2. Are you on the Free Pricing Tier of OMS/Log Analytics? The Free plan allows for up to five unique Service Map servers. Any subsequent servers won't show up in Service Map, even if the prior five are no longer sending data.

3. Is your server sending log and perf data to OMS? Go to Log Search and run the following query for your computer:

   ```
   * Computer="<your computer name here>" | measure count() by Type
   ```

Did you get a variety of events in the results? Is the data recent? If so, your OMS Agent is operating correctly and communicating to the OMS service. If not, check the OMS Agent on your server: OMS Agent for Windows troubleshooting. OMS Agent for Linux troubleshooting.

Server shows in Service Map, but has no processes

If you see your server in Service Map, but it has no process or connection data, that indicates that the Dependency Agent is installed and running, but the kernel driver didn't load. To find out why your driver didn't load, check the wrapper.log file (Windows) or service.log file (Linux). The last lines of the file should indicate why (e.g. kernel not supported, which can happen on Linux if you updated your kernel) the kernel didn't load.

Windows: C:\Program Files\Microsoft Dependency Agent\logs\wrapper.log

Linux: /var/opt/microsoft/dependency-agent/log/service.log

Data collection

You can expect each agent to transmit roughly 25 MB per day, depending on how complex your system dependencies are. Service Map dependency data is sent by each agent every 15 seconds.

The Dependency Agent typically consumes 0.1% of system memory and 0.1% of system CPU.

Supported operating systems

The following sections list the supported operating systems for the Dependency Agent. 32-bit architectures are not supported for any operating system.

Windows Server

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Windows Desktop

- WIndows 10
- Windows 8.1
- Windows 8
- Windows 7

Red Hat Enterprise Linux, CentOS Linux, and Oracle Linux (with RHEL Kernel)

- Only default and SMP Linux kernel releases are supported.
- Non-standard kernel releases, such as PAE and Xen, are not supported for any Linux distribution. For example, a system with the release string of "2.6.16.21-0.8-xen" is not supported.
- Custom kernels, including recompiles of standard kernels, are not supported
- Centos Plus kernel is not supported.
- Oracle Unbreakable Kernel (UEK) is covered in a different section below.

Red Hat Linux 7

OS VERSION	KERNEL VERSION
7.0	3.10.0-123
7.1	3.10.0-229
7.2	3.10.0-327
7.3	3.10.0-514

Red Hat Linux 6

OS VERSION	KERNEL VERSION
6.0	2.6.32-71
6.1	2.6.32-131
6.2	2.6.32-220

OS VERSION	KERNEL VERSION
6.3	2.6.32-279
6.4	2.6.32-358
6.5	2.6.32-431
6.6	2.6.32-504
6.7	2.6.32-573
6.8	2.6.32-642

Red Hat Linux 5

OS VERSION	KERNEL VERSION
5.8	2.6.18-308
5.9	2.6.18-348
5.10	2.6.18-371
5.11	2.6.18-398 2.6.18-400 2.6.18-402 2.6.18-404 2.6.18-406 2.6.18-407 2.6.18-408 2.6.18-409 2.6.18-410 2.6.18-411 2.6.18-412 2.6.18-416 2.6.18-417 2.6.18-419

Oracle Enterprise Linux w/ Unbreakable Kernel (UEK)

Oracle Linux 6

OS VERSION	KERNEL VERSION
6.2	Oracle 2.6.32-300 (UEK R1)
6.3	Oracle 2.6.39-200 (UEK R2)
6.4	Oracle 2.6.39-400 (UEK R2)
6.5	Oracle 2.6.39-400 (UEK R2 i386)
6.6	Oracle 2.6.39-400 (UEK R2 i386)

Oracle Linux 5

OS VERSION	KERNEL VERSION
5.8	Oracle 2.6.32-300 (UEK R1)
5.9	Oracle 2.6.39-300 (UEK R2)
5.10	Oracle 2.6.39-400 (UEK R2)
5.11	Oracle 2.6.39-400 (UEK R2)

SUSE Linux Enterprise Server

SUSE Linux 11

OS VERSION	KERNEL VERSION
11	2.6.27
11 SP1	2.6.32
11 SP2	3.0.13
11 SP3	3.0.76
11 SP4	3.0.101

SUSE Linux 10

OS VERSION	KERNEL VERSION
10 SP4	2.6.16.60

Diagnostic and usage data

Microsoft automatically collects usage and performance data through your use of the Service Map service. Microsoft uses this Data to provide and improve the quality, security and integrity of the Service Map service. Data includes information about the configuration of your software, like operating system and version, and also includes IP address, DNS name, and Workstation name in order to provide accurate and efficient troubleshooting capabilities. We do not collect names, addresses, or other contact information.

For more information on data collection and usage, please see the Microsoft Online Services Privacy Statement.

Next steps

- Learn how to use Service Map once it has been deployed and configured.

Azure networking monitoring solutions in Log Analytics

3/23/2017 • 7 min to read • Edit Online

Log Analytics offers the following solutions for monitoring your networks:

- Network Performance Monitor (NPM) to
  - Monitor the health of your network
- Azure Application Gateway analytics to review
  - Azure Application Gateway logs
  - Azure Application Gateway metrics
- Azure Network Security Group analytics to review
  - Azure Network Security Group logs

Network Performance Monitor (NPM)

The Network Performance Monitor management solution is a network monitoring solution, that monitors the health, availability and reachability of networks. It is used to monitor connectivity between:

- public cloud and on-premises
- data centers and user locations (branch offices)
- subnets hosting various tiers of a multi-tiered application.

For more information, see Network Performance Monitor.

Azure Application Gateway and Network Security Group analytics

To use the solutions:

1. Add the management solution to Log Analytics, and
2. Enable diagnostics to direct the diagnostics to a Log Analytics workspace. It is not necessary to write the logs to Azure Blob storage.

You can enable diagnostics and the corresponding solution for either one or both of Application Gateway and Networking Security Groups.

If you do not enable diagnostic logging for a particular resource type, but install the solution, the dashboard blades for that resource are blank and display an error message.

> **NOTE**
> In January 2017, the supported way of sending logs from Application Gateways and Network Security Groups to Log Analytics changed. If you see the **Azure Networking Analytics (deprecated)** solution, refer to migrating from the old Networking Analytics solution for steps you need to follow.

Review Azure networking data collection details

The Azure Application Gateway analytics and the Network Security Group analytics management solutions collect diagnostics logs directly from Azure Application Gateways and Network Security Groups. It is not necessary to write

the logs to Azure Blob storage and no agent is required for data collection.

The following table shows data collection methods and other details about how data is collected for Azure Application Gateway analytics and the Network Security Group analytics.

PLATFORM	DIRECT AGENT	SYSTEMS CENTER OPERATIONS MANAGER AGENT	AZURE	OPERATIONS MANAGER REQUIRED?	OPERATIONS MANAGER AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Azure	✗	✗	●	✗	✗	when logged

Azure Application Gateway analytics solution in Log Analytics

The following logs are supported for Application Gateways:

- ApplicationGatewayAccessLog
- ApplicationGatewayPerformanceLog
- ApplicationGatewayFirewallLog

The following metrics are supported for Application Gateways:

- 5 minute throughput

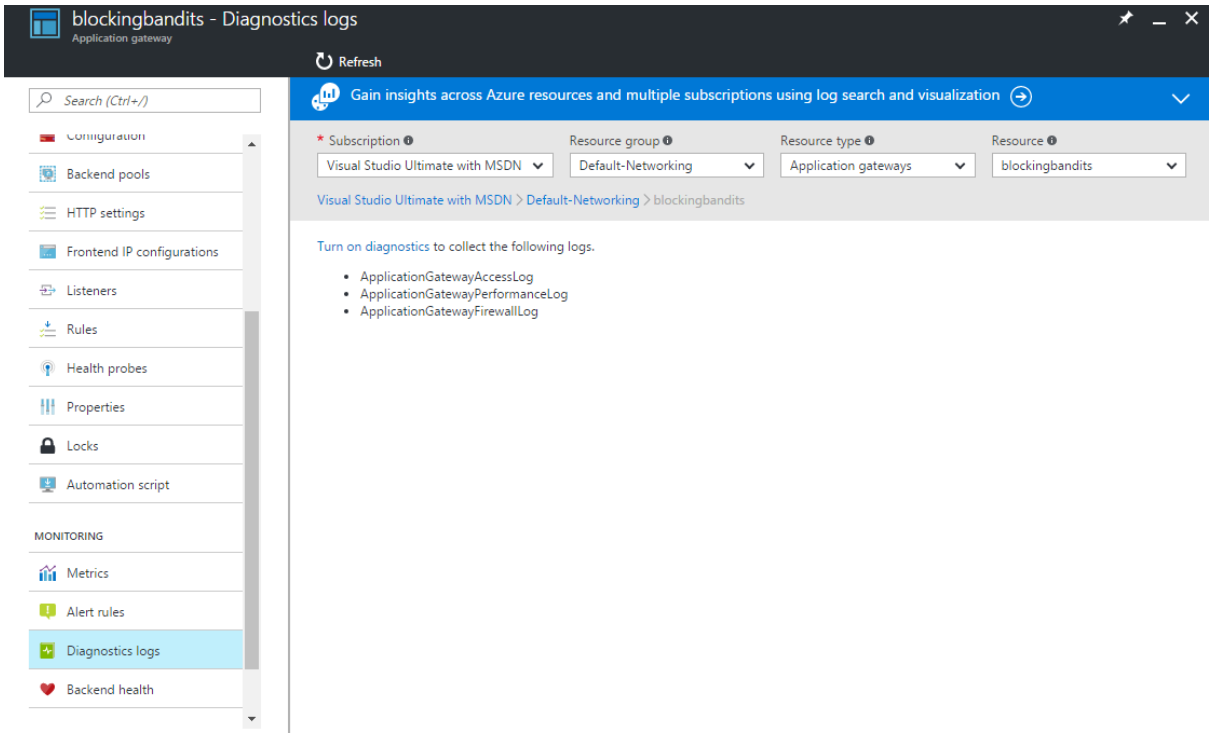
Install and configure the solution

Use the following instructions to install and configure the Azure Application Gateway analytics solution:

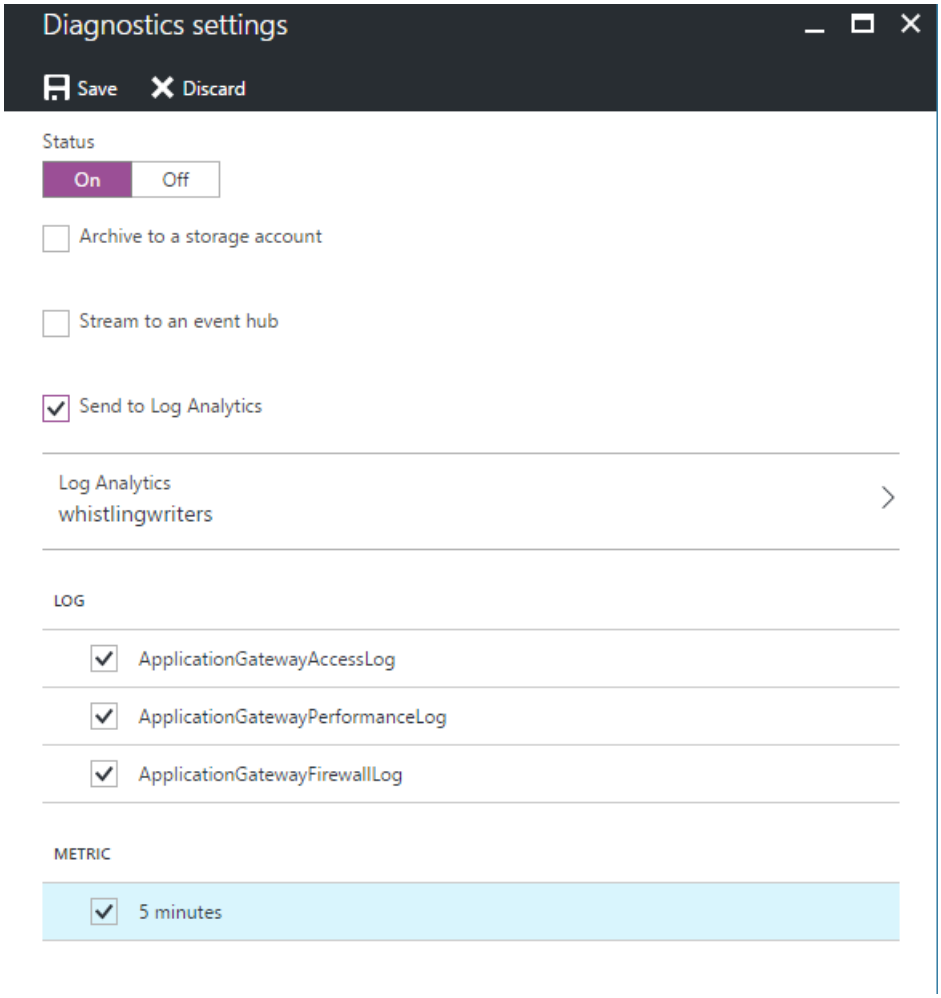
1. Enable the Azure Application Gateway analytics solution from Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery.
2. Enable diagnostics logging for the Application Gateways you want to monitor.

Enable Azure Application Gateway diagnostics in the portal

1. In the Azure portal, navigate to the Application Gateway resource to monitor
2. Select *Diagnostics logs* to open the following page



3. Click *Turn on diagnostics* to open the following page



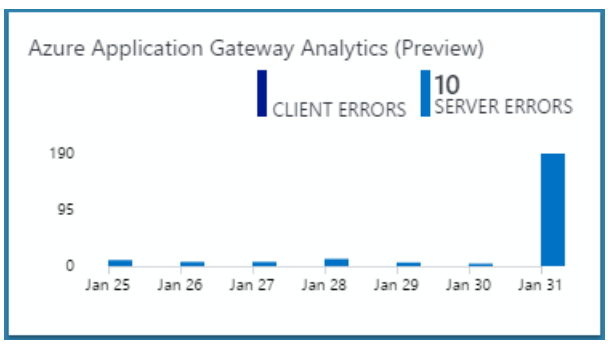
4. To turn on diagnostics, click *On* under *Status*
5. Click the checkbox for *Send to Log Analytics*
6. Select an existing Log Analytics workspace, or create a workspace
7. Click the checkbox under **Log** for each of the log types to collect
8. Click *Save* to enable the logging of diagnostics to Log Analytics

Enable Azure network diagnostics using PowerShell

The following PowerShell script provides an example of how to enable diagnostic logging for application gateways.

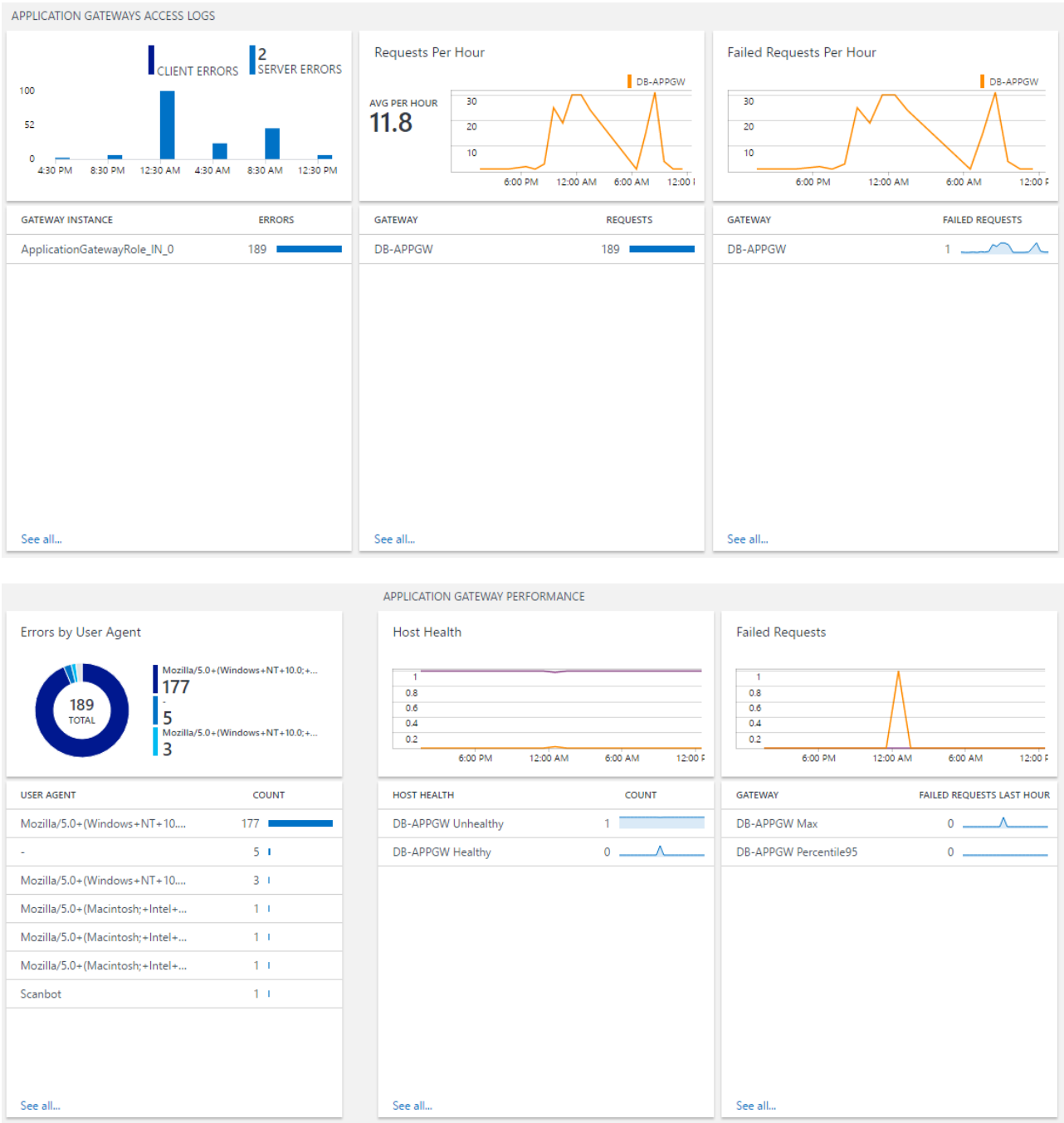
```
$workspaceId = "/subscriptions/d2e37fee-1234-40b2-5678-0b2199de3b50/resourcegroups/oi-default-east-
us/providers/microsoft.operationalinsights/workspaces/rollingbaskets"

$gateway = Get-AzureRmApplicationGateway -Name 'ContosoGateway'

Set-AzureRmDiagnosticSetting -ResourceId $gateway.ResourceId  -WorkspaceId $workspaceId -Enabled $true
```

Use Azure Application Gateway analytics



After you click the **Azure Application Gateway analytics** tile on the Overview, you can view summaries of your logs and then drill in to details for the following categories:

- Application Gateway Access logs
  - Client and server errors for Application Gateway access logs
  - Requests per hour for each Application Gateway
  - Failed requests per hour for each Application Gateway
  - Errors by user agent for Application Gateways
- Application Gateway performance
  - Host health for Application Gateway
  - Maximum and 95th percentile for Application Gateway failed requests



On the **Azure Application Gateway analytics** dashboard, review the summary information in one of the blades, and then click one to view detailed information on the log search page.

On any of the log search pages, you can view results by time, detailed results, and your log search history. You can also filter by facets to narrow the results.

Azure Network Security Group analytics solution in Log Analytics

The following logs are supported for network security groups:

- NetworkSecurityGroupEvent
- NetworkSecurityGroupRuleCounter

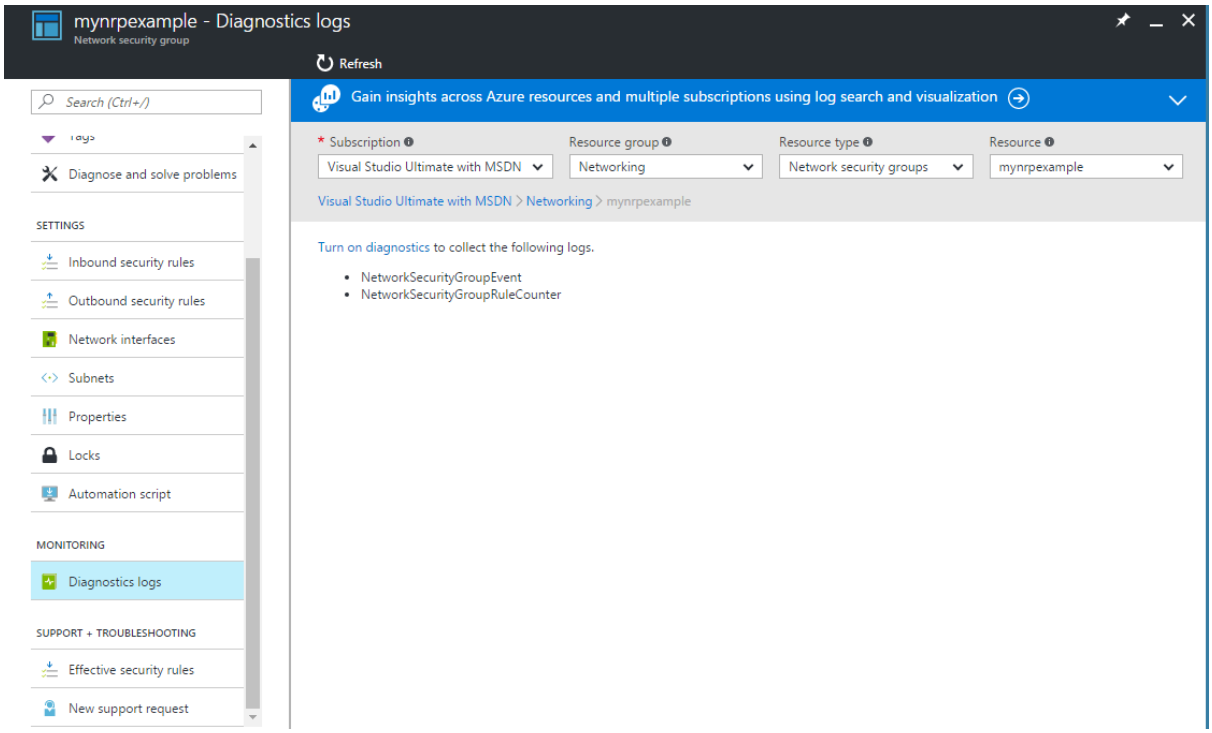
Install and configure the solution

Use the following instructions to install and configure the Azure Networking Analytics solution:

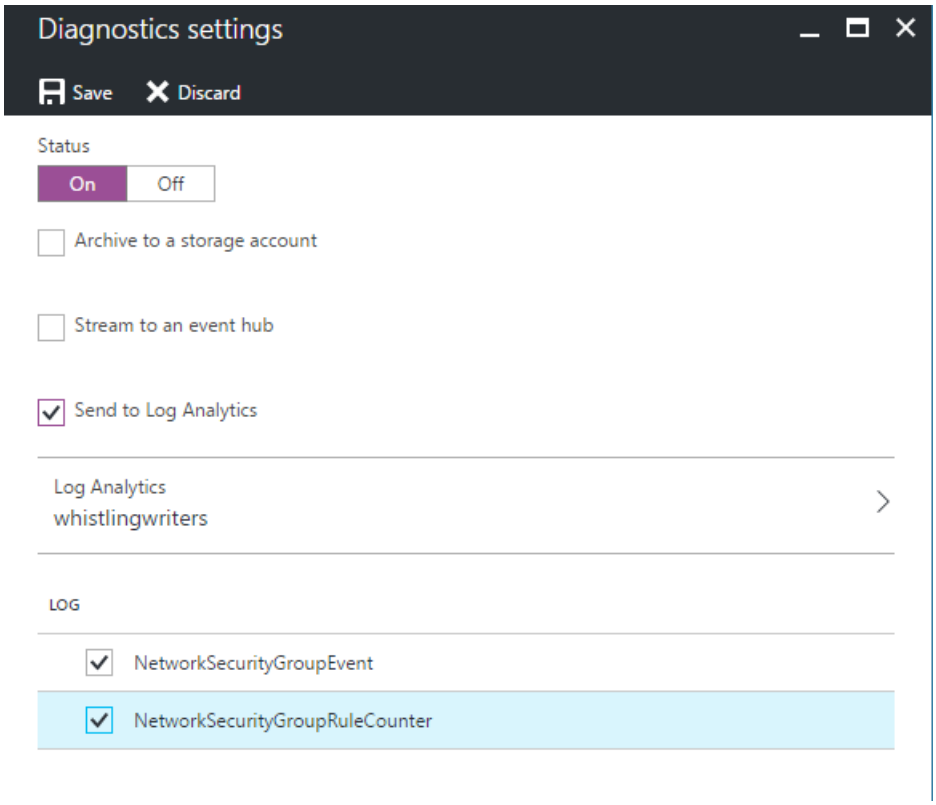
1. Enable the Azure Network Security Group analytics solution from Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery.
2. Enable diagnostics logging for the Network Security Group resources you want to monitor.

Enable Azure network security group diagnostics in the portal

1. In the Azure portal, navigate to the Network Security Group resource to monitor
2. Select *Diagnostics logs* to open the following page



3. Click *Turn on diagnostics* to open the following page



4. To turn on diagnostics, click *On* under *Status*
5. Click the checkbox for *Send to Log Analytics*
6. Select an existing Log Analytics workspace, or create a workspace
7. Click the checkbox under **Log** for each of the log types to collect
8. Click *Save* to enable the logging of diagnostics to Log Analytics

Enable Azure network diagnostics using PowerShell

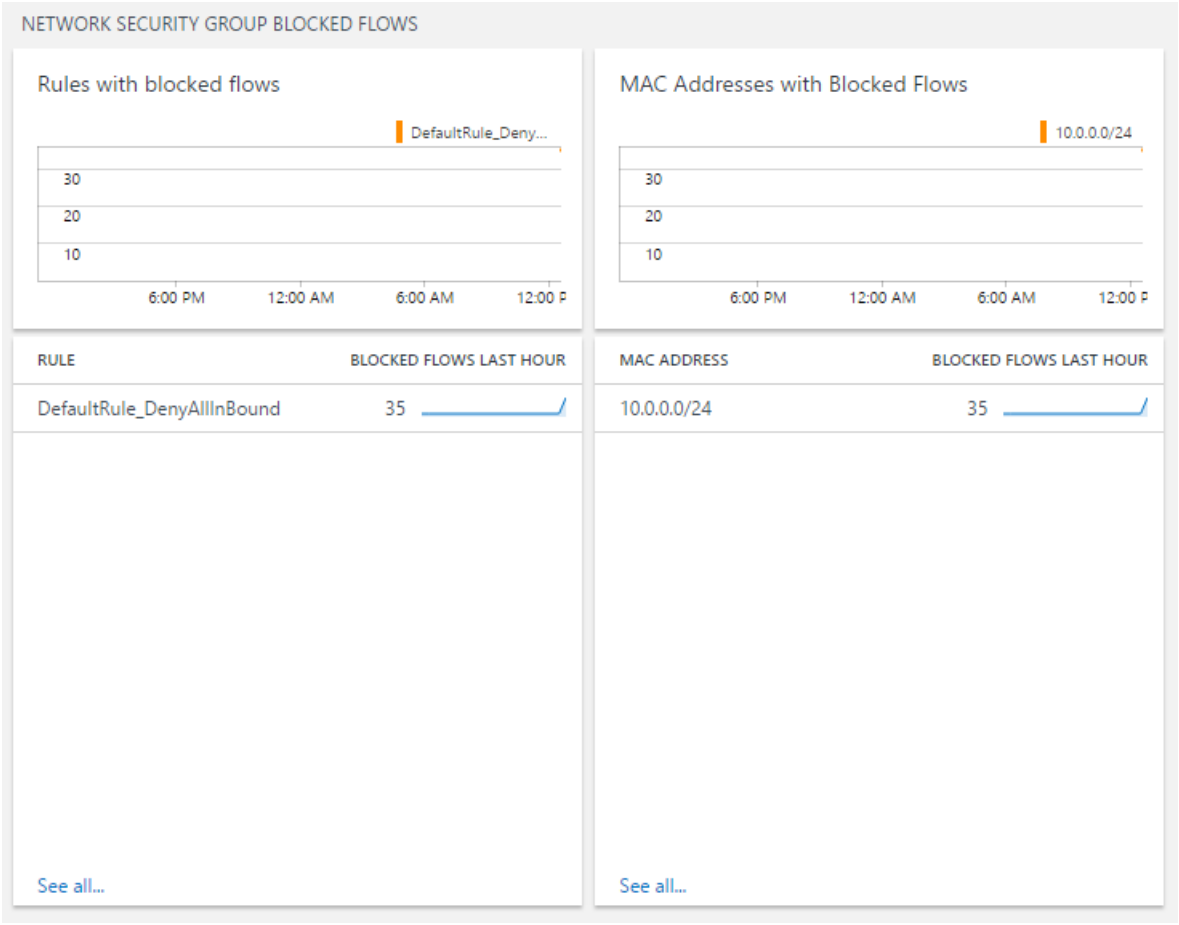
The following PowerShell script provides an example of how to enable diagnostic logging for network security groups

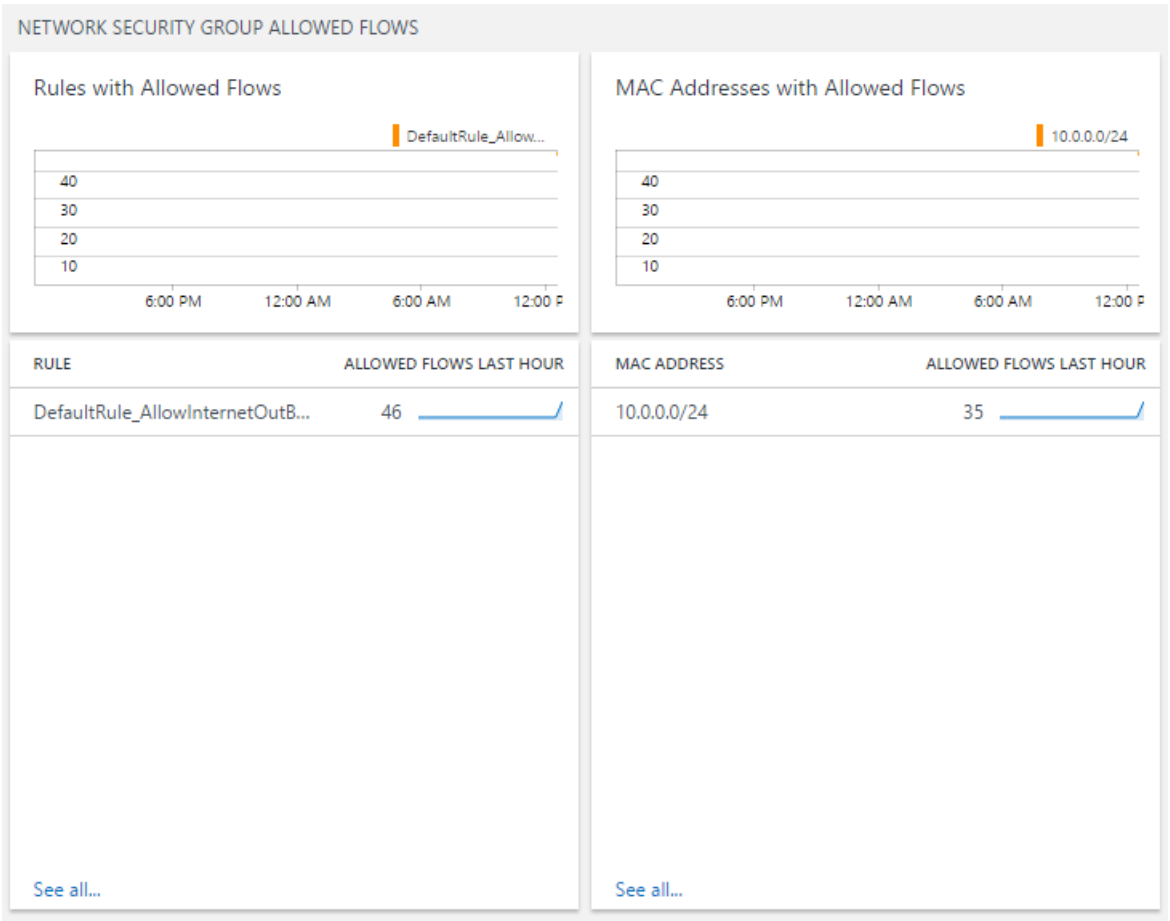
```
$workspaceId = "/subscriptions/d2e37fee-1234-40b2-5678-0b2199de3b50/resourcegroups/oi-default-east-us/providers/microsoft.operationalinsights/workspaces/rollingbaskets"

$nsg = Get-AzureRmNetworkSecurityGroup -Name 'ContosoNSG'

Set-AzureRmDiagnosticSetting -ResourceId $nsg.ResourceId  -WorkspaceId $workspaceId -Enabled $true
```

Use Azure Network Security Group analytics

After you click the **Azure Network Security Group analytics** tile on the Overview, you can view summaries of your logs and then drill in to details for the following categories:

- Network security group blocked flows
  - Network security group rules with blocked flows
  - MAC addresses with blocked flows
- Network security group allowed flows
  - Network security group rules with allowed flows
  - MAC addresses with allowed flows





On the **Azure Network Security Group analytics** dashboard, review the summary information in one of the blades, and then click one to view detailed information on the log search page.

On any of the log search pages, you can view results by time, detailed results, and your log search history. You can also filter by facets to narrow the results.

Migrating from the old Networking Analytics solution

In January 2017, the supported way of sending logs from Azure Application Gateways and Azure Network Security Groups to Log Analytics changed. These changes provide the following advantages:

- Logs are written directly to Log Analytics without the need to use a storage account
- Less latency from the time when logs are generated to them being available in Log Analytics
- Fewer configuration steps
- A common format for all types of Azure diagnostics

To use the updated solutions:

1. Configure diagnostics to be sent directly to Log Analytics from Azure Application Gateways
2. Configure diagnostics to be sent directly to Log Analytics from Azure Network Security Groups
3. Enable the *Azure Application Gateway Analytics* and the *Azure Network Security Group Analytics* solution by using the process described in Add Log Analytics solutions from the Solutions Gallery
4. Update any saved queries, dashboards, or alerts to use the new data type

   - Type is to AzureDiagnostics. You can use the ResourceType to filter to Azure networking logs.

INSTEAD OF:	USE:
`Type=NetworkApplicationgateways OperationName=ApplicationGatewayAccess`	`Type=AzureDiagnostics ResourceType=APPLICATIONGATEWAYS OperationName=ApplicationGatewayAccess`
`Type=NetworkApplicationgateways OperationName=ApplicationGatewayPerformance`	`Type=AzureDiagnostics ResourceType=APPLICATIONGATEWAYS OperationName=ApplicationGatewayPerformance`
`Type=NetworkSecuritygroups`	`Type=AzureDiagnostics ResourceType=NETWORKSECURITYGROUPS`

   - For any field that has a suffix of _s, _d, or _g in the name, change the first character to lower case
   - For any field that has a suffix of _o in name, the data is split into individual fields based on the nested field names.
5. Remove the *Azure Networking Analytics (Deprecated)* solution.
   - If you are using PowerShell, use

```
Set-AzureOperationalInsightsIntelligencePack -ResourceGroupName <resource group that the workspace is in> -WorkspaceName <name of the log analytics workspace> -IntelligencePackName "AzureNetwork" -Enabled $false
```

Data collected before the change is not visible in the new solution. You can continue to query for this data using the old Type and field names.

Troubleshooting

Troubleshoot Azure Diagnostics

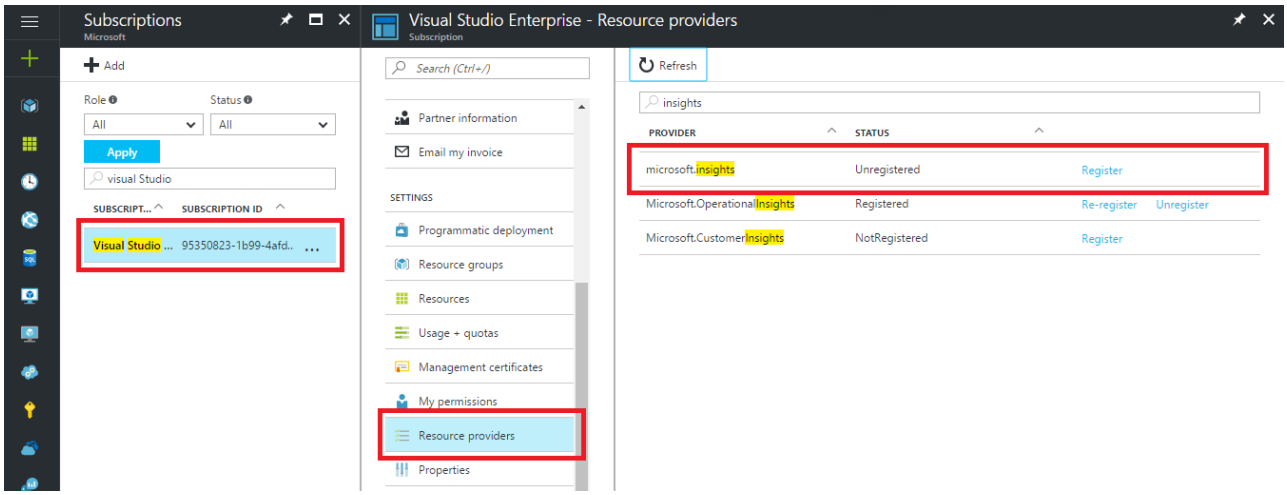
If you receive the following error message, the Microsoft.insights resource provider is not registered:

```
Failed to update diagnostics for 'resource'. {"code":"Forbidden","message":"Please register the subscription 'subscription id' with Microsoft.Insights."}
```

To register the resource provider, perform the following steps in the Azure portal:

1. In the navigation pane on the left, click *Subscriptions*
2. Select the subscription identified in the error message

3. Click *Resource Providers*
4. Find the *Microsoft.insights* provider
5. Click the *Register* link



Once the *Microsoft.insights* resource provider is registered, retry configuring diagnostics.

In PowerShell, if you receive the following error message, you need to update your version of PowerShell:

```
Set-AzureRmDiagnosticSetting : A parameter cannot be found that matches parameter name 'WorkspaceId'.
```

Update your version of PowerShell to the November 2016 (v2.3.0), or later, release using the instructions in the Get started with Azure PowerShell cmdlets article.

Next steps

- Use Log searches in Log Analytics to view detailed Azure diagnostics data.

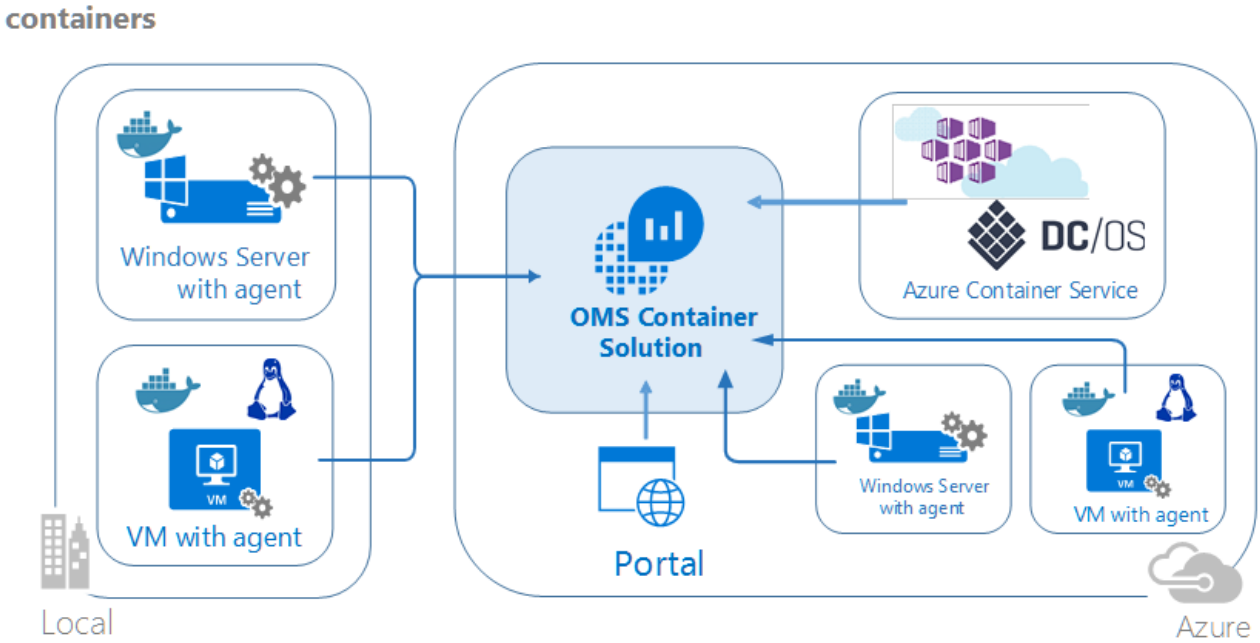
Containers (Preview) solution Log Analytics

5/3/2017 • 9 min to read • Edit Online

This article describes how to set up and use the Containers solution in Log Analytics, which helps you view and manage your Docker and Windows container hosts in a single location. Docker is a software virtualization system used to create containers that automate software deployment to their IT infrastructure.

With the solution, you can see which containers are running on your container hosts and what images are running in the containers. You can view detailed audit information showing commands used with containers. And, you can troubleshoot containers by viewing and searching centralized logs without having to remotely view Docker or Windows hosts. You can find containers that may be noisy and consuming excess resources on a host. And, you can view centralized CPU, memory, storage, and network usage and performance information for containers. On computers running Windows, you can centralize and compare logs from Windows Server, Hyper-V, and Docker containers.

The following diagram shows the relationships between various container hosts and agents with OMS.



Installing and configuring the solution

Use the following information to install and configure the solution.

Add the Containers solution to your OMS workspace from Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery.

There are a few ways to install and use Docker with OMS:

- On supported Linux operating systems, install and run Docker and then install and configure the OMS Agent for Linux.
- On CoreOS, you cannot run the OMS Agent for Linux. Instead, you run a containerized version of the OMS Agent for Linux.
- On Windows Server 2016 and Windows 10, install the Docker Engine and client then connect an agent to gather information and send it to Log Analytics.

You can review the supported Docker and Linux operating system versions for your container host on GitHub.

If you have a Kubernetes cluster using the Azure Container Service, learn more at Monitor an Azure Container Service cluster with Microsoft Operations Management Suite (OMS).

If you have an Azure Container Service DC/OS cluster, learn more at Monitor an Azure Container Service DC/OS cluster with Operations Management Suite.

Review the Docker Engine on Windows article for additional information about how to install and configure your Docker Engines on computers running Windows.

> **IMPORTANT**
> Docker must be running **before** you install the OMS Agent for Linux on your container hosts. If you've already installed the agent before installing Docker, you'll need to reinstall the OMS Agent for Linux. For more information about Docker, see the Docker website.

You need the following settings configured on your container hosts before you can monitor containers.

Configure settings for a Linux container host

The following x64 Linux distributions are supported as container hosts:

- Ubuntu 14.04 LTS, 16.04 LTS
- CoreOS(stable)
- Amazon Linux 2016.09.0
- openSUSE 13.2
- CentOS 7
- SLES 12
- RHEL 7.2

After you've installed Docker, use the following settings for your container host to configure the agent for use with Docker. You'll need your OMS workspace ID and key.

For all Linux container hosts except CoreOS

- Follow the instructions at Steps to install the OMS Agent for Linux.

For all Linux container hosts including CoreOS

Start the OMS container that you want to monitor. Modify and use the following example.

```
sudo docker run --privileged -d -v /var/run/docker.sock:/var/run/docker.sock -e WSID="your workspace id" -e
KEY="your key" -h=`hostname` -p 127.0.0.1:25225:25225 --name="omsagent" --restart=always microsoft/oms
```

Switching from using an installed Linux agent to one in a container

If you previously used the directly-installed agent and want to instead use an agent running in a container, you must first remove OMSAgent. See Steps to install the OMS Agent for Linux.

Supported Windows versions

- Windows Server 2016
- Windows 10 Anniversary Edition (Professional or Enterprise)

Docker versions supported on Windows

- Docker 1.12 – 1.13

Preparation before installing agents

Before you install agents on computers running Windows, you need to configure the Docker service. The configuration allows the Windows agent or the Log Analytics virtual machine extension to use the Docker TCP socket so that the agents can access the Docker daemon remotely and to capture data for monitoring.

For more information about configuring the Docker daemon with Windows, see Docker Engine on Windows.

To start Docker and verify its configuration

1. In Windows PowerShell, enable TCP pipe and named pipe.

```
Stop-Service docker
dockerd --unregister-service
dockerd -H npipe:// -H 0.0.0.0:2375 --register-service
Start-Service docker
```

2. Verify your configuration with netstat. You should see port 2375.

```
PS C:\Users\User1> netstat -a | sls 2375

TCP    127.0.0.1:2375         Win2016TP5:0           LISTENING
TCP    127.0.0.1:2375         Win2016TP5:49705       ESTABLISHED
TCP    127.0.0.1:2375         Win2016TP5:49706       ESTABLISHED
TCP    127.0.0.1:2375         Win2016TP5:49707       ESTABLISHED
TCP    127.0.0.1:2375         Win2016TP5:49708       ESTABLISHED
TCP    127.0.0.1:49705        Win2016TP5:2375        ESTABLISHED
TCP    127.0.0.1:49706        Win2016TP5:2375        ESTABLISHED
TCP    127.0.0.1:49707        Win2016TP5:2375        ESTABLISHED
TCP    127.0.0.1:49708        Win2016TP5:2375        ESTABLISHED
```

Install Windows agents

To enable Windows and Hyper-V container monitoring, install agents on Windows computers that are container hosts. For computers running Windows in your on-premises environment, see Connect Windows computers to Log Analytics. For virtual machines running in Azure, connect them to Log Analytics using the virtual machine extension.

To verify that the Containers solution is set correctly:

- Check whether the management pack was download properly, look for *ContainerManagement.xxx*.
  - The files should be in the C:\Program Files\Microsoft Monitoring Agent\Agent\Health Service State\Management Packs folder.
- Verify that the OMS Workspace ID is correct by going to **Control Panel** > **System and Security**.
  - Open **Microsoft Monitoring Agent** and verify that the workspace information is correct.

Containers data collection details

The Containers solution collects various performance metrics and log data from container hosts and containers using agents that you enable.

The following table shows data collection methods and other details about how data is collected for Containers.

PLATFORM	OMS AGENT FOR LINUX	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Linux						every 3 minutes

PLATFORM	WINDOWS AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows						every 3 minutes

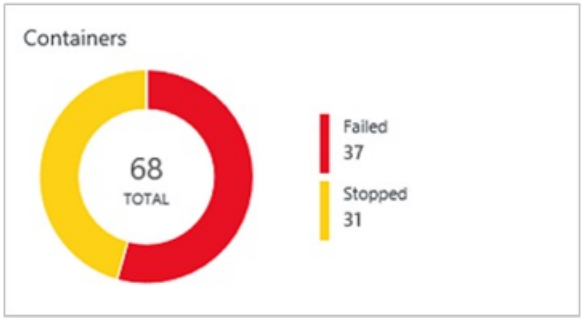
PLATFORM	LOG ANALYTICS VM EXTENSION	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Azure						every 3 minutes

The following table show examples of data types collected by the Containers solution and the data types that are used in Log Searches and results.

DATA TYPE	DATA TYPE IN LOG SEARCH	FIELDS
Performance for hosts and containers	`Type=Perf`	Computer, ObjectName, CounterName (%Processor Time, Disk Reads MB, Disk Writes MB, Memory Usage MB, Network Receive Bytes, Network Send Bytes, Processor Usage sec, Network), CounterValue,TimeGenerated, CounterPath, SourceSystem
Container inventory	`Type=ContainerInventory`	TimeGenerated, Computer, container name, ContainerHostname, Image, ImageTag, ContinerState, ExitCode, EnvironmentVar, Command, CreatedTime, StartedTime, FinishedTime, SourceSystem, ContainerID, ImageID
Container image inventory	`Type=ContainerImageInventory`	TimeGenerated, Computer, Image, ImageTag, ImageSize, VirtualSize, Running, Paused, Stopped, Failed, SourceSystem, ImageID, TotalContainer
Container log	`Type=ContainerLog`	TimeGenerated, Computer, image ID, container name, LogEntrySource, LogEntry, SourceSystem, ContainerID
Container service log	`Type=ContainerServiceLog`	TimeGenerated, Computer, TimeOfCommand, Image, Command, SourceSystem, ContainerID

Monitor containers

After you have the solution enabled in the OMS portal, you'll see the **Containers** tile showing summary information about your container hosts and the containers running in hosts.



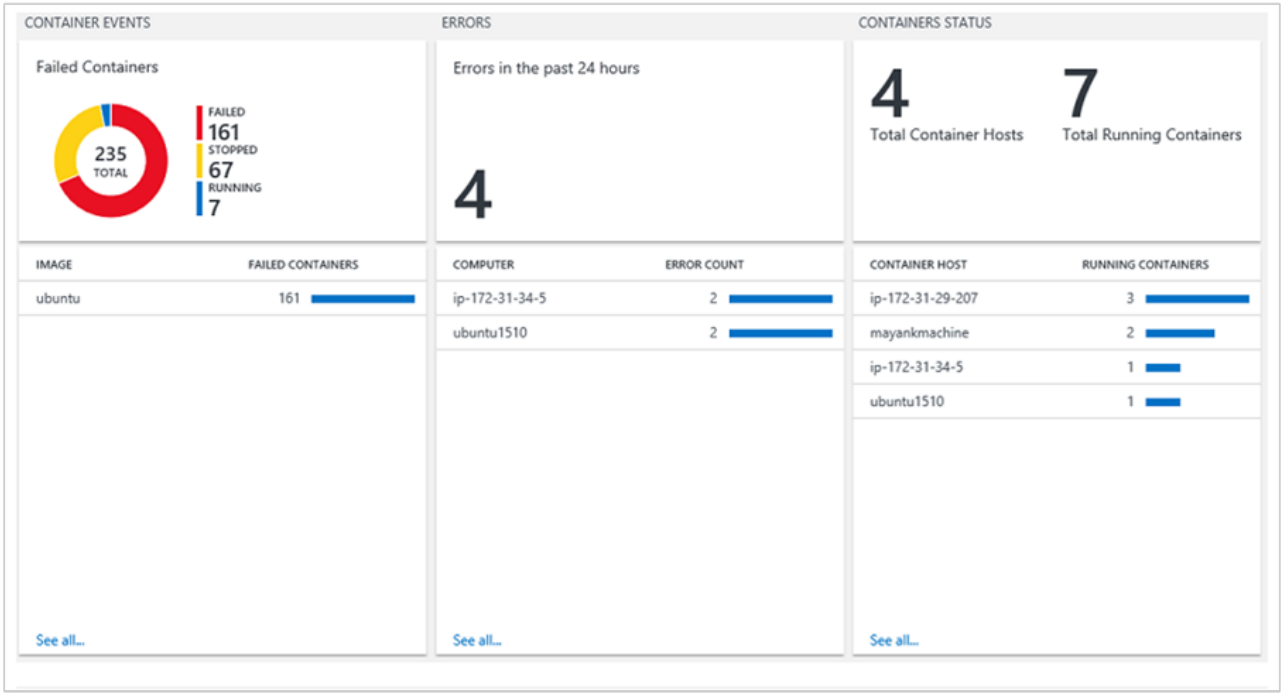
The tile shows an overview of how many containers you have in the environment and whether they're failed, running, or stopped.

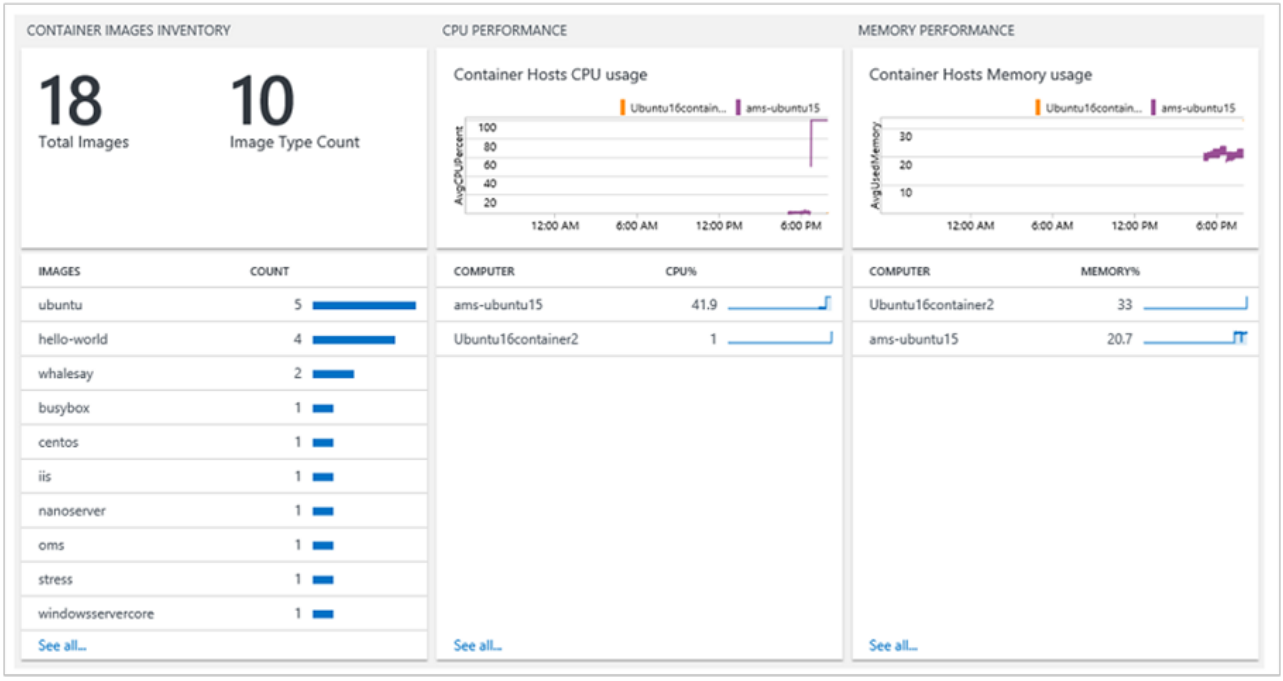
Using the Containers dashboard

Click the **Containers** tile. From there you'll see views organized by:

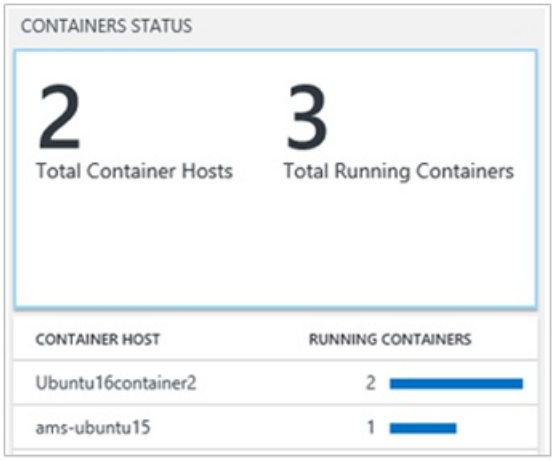
- Container Events
- Errors
- Containers Status
- Container Image Inventory
- CPU and Memory performance

Each pane in the dashboard is a visual representation of a search that is run on collected data.

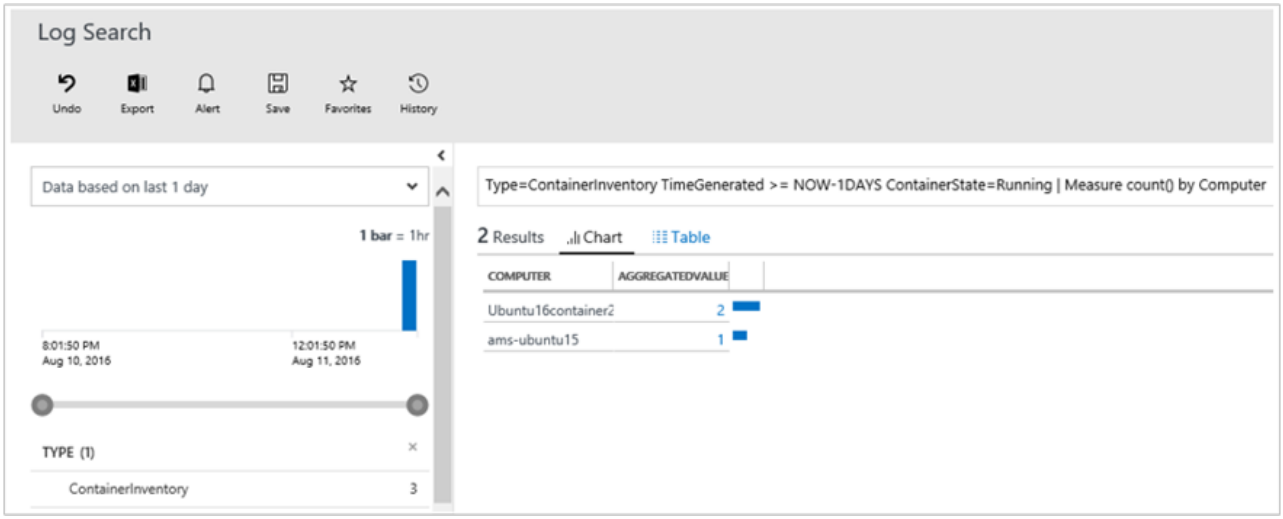




In the **Container Status** blade, click to top area, as shown below.



Log Search opens, displaying information about the hosts and containers running in them.



From here, you can edit the search query to modify it to find the specific information you're interested in. For more information about Log Searches, see Log searches in Log Analytics.

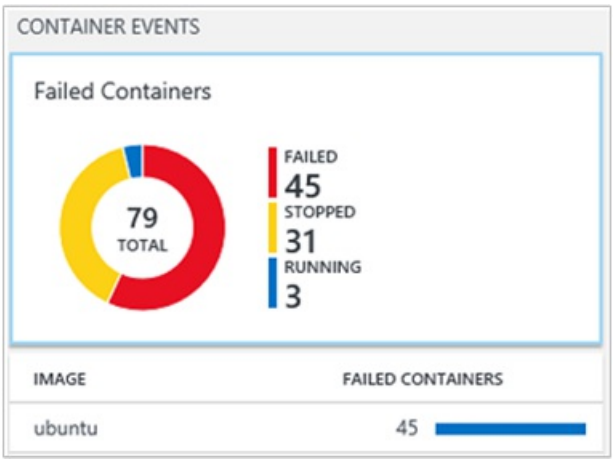
For example, you can modify the search query so that it shows all the stopped containers instead of the running containers by changing **Running** to **Stopped** in the search query.

Troubleshoot by finding a failed container

OMS marks a container as **Failed** if it has exited with a non-zero exit code. You can see an overview of the errors and failures in the environment in the **Failed Containers** blade.

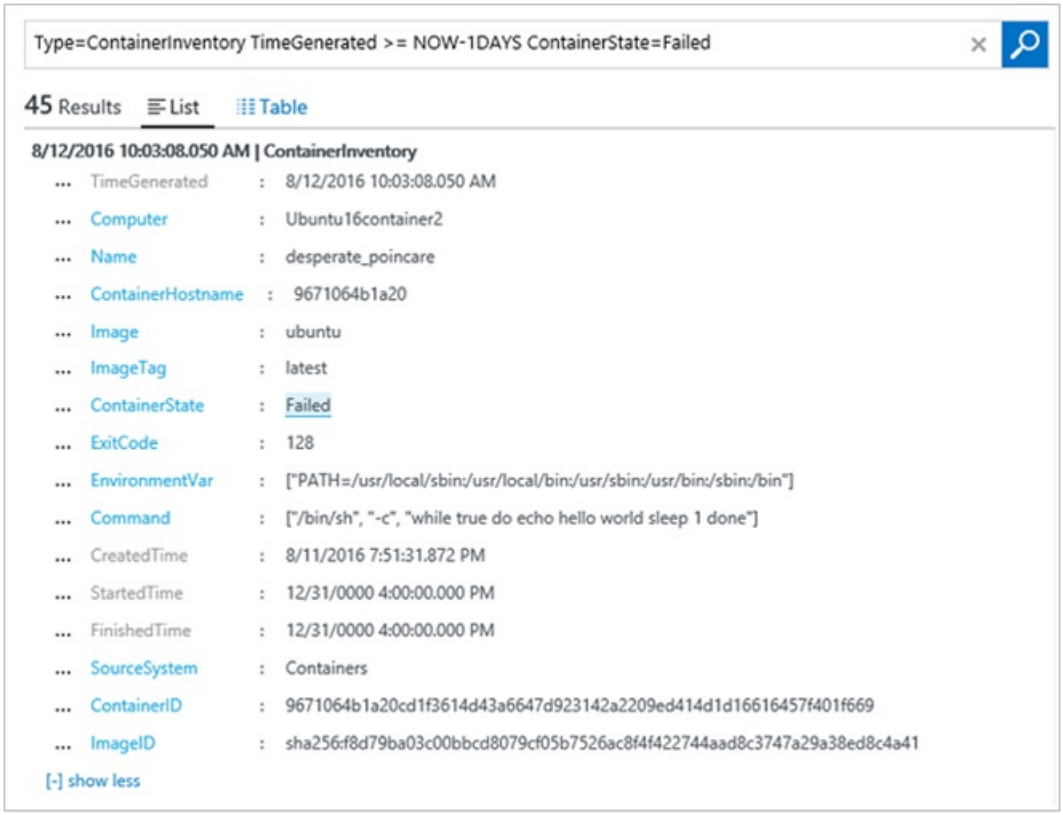
To find failed containers

1. Click the **Container Events** blade.

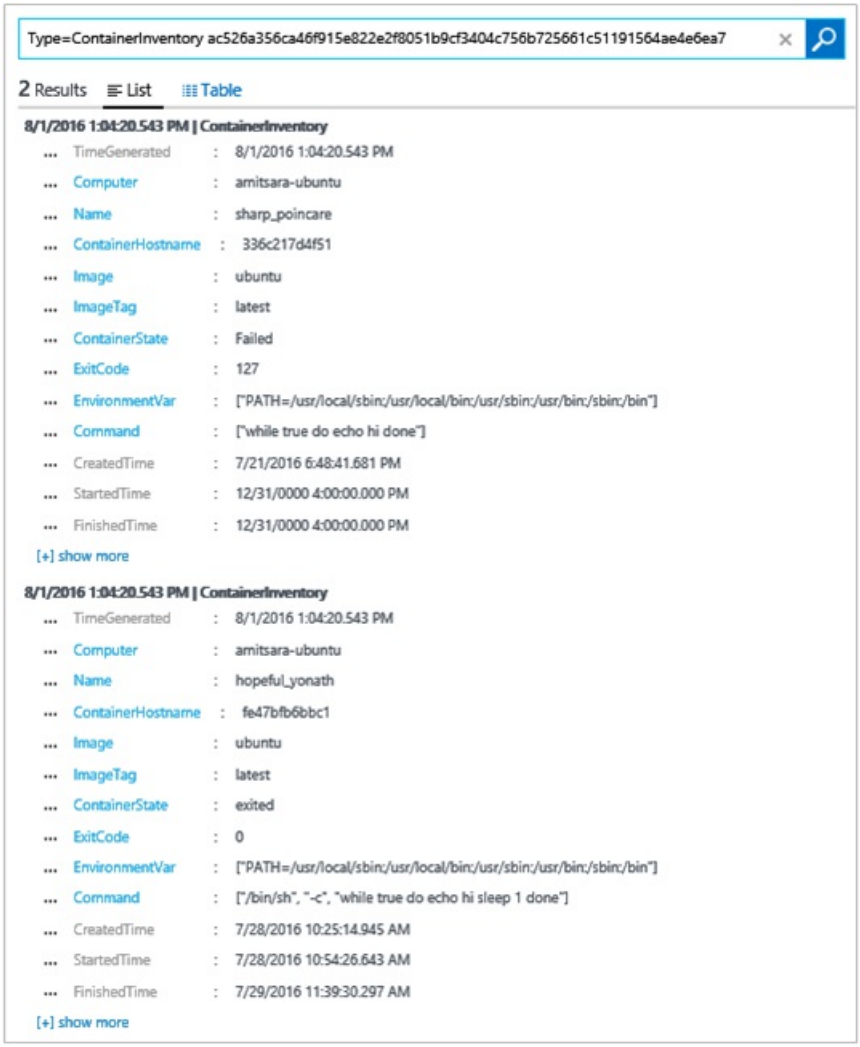


2. Log Search opens, displaying the status of containers, similar to the following.

3. Next, click the failed value to view additional information such as image size and number of stopped and failed images. Expand **show more** to view the image ID.



4. Next, find the container that is running this image. Type the following into the search query.
`Type=ContainerInventory <ImageID>` This displays the logs. You can scroll to see the failed container.



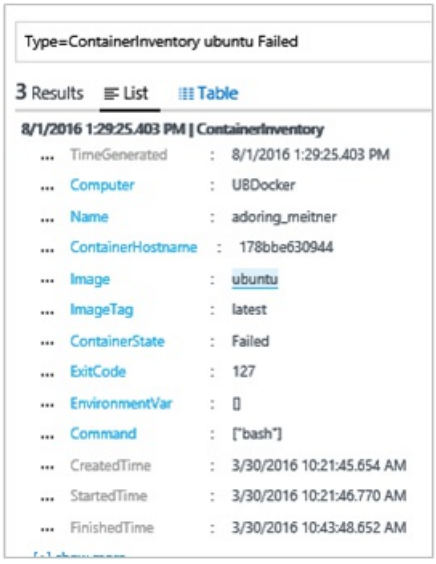
Search logs for container data

When you're troubleshooting a specific error, it can help to see where it is occurring in your environment. The following log types will help you create queries to return the information you want.

- **ContainerInventory** – Use this type when you want information about container location, what their names are, and what images they're running.
- **ContainerImageInventory** – Use this type when you're trying to find information organized by image and to view image information such as image IDs or sizes.
- **ContainerLog** – Use this type when you want to find specific error log information and entries.
- **ContainerServiceLog** – Use this type when you're trying to find audit trail information for the Docker daemon, such as start, stop, delete, or pull commands.

To search logs for container data

- Choose an image that you know has failed recently and find the error logs for it. Start by finding a container name that is running that image with a **ContainerInventory** search. For example, search for `Type=ContainerInventory ubuntu Failed`

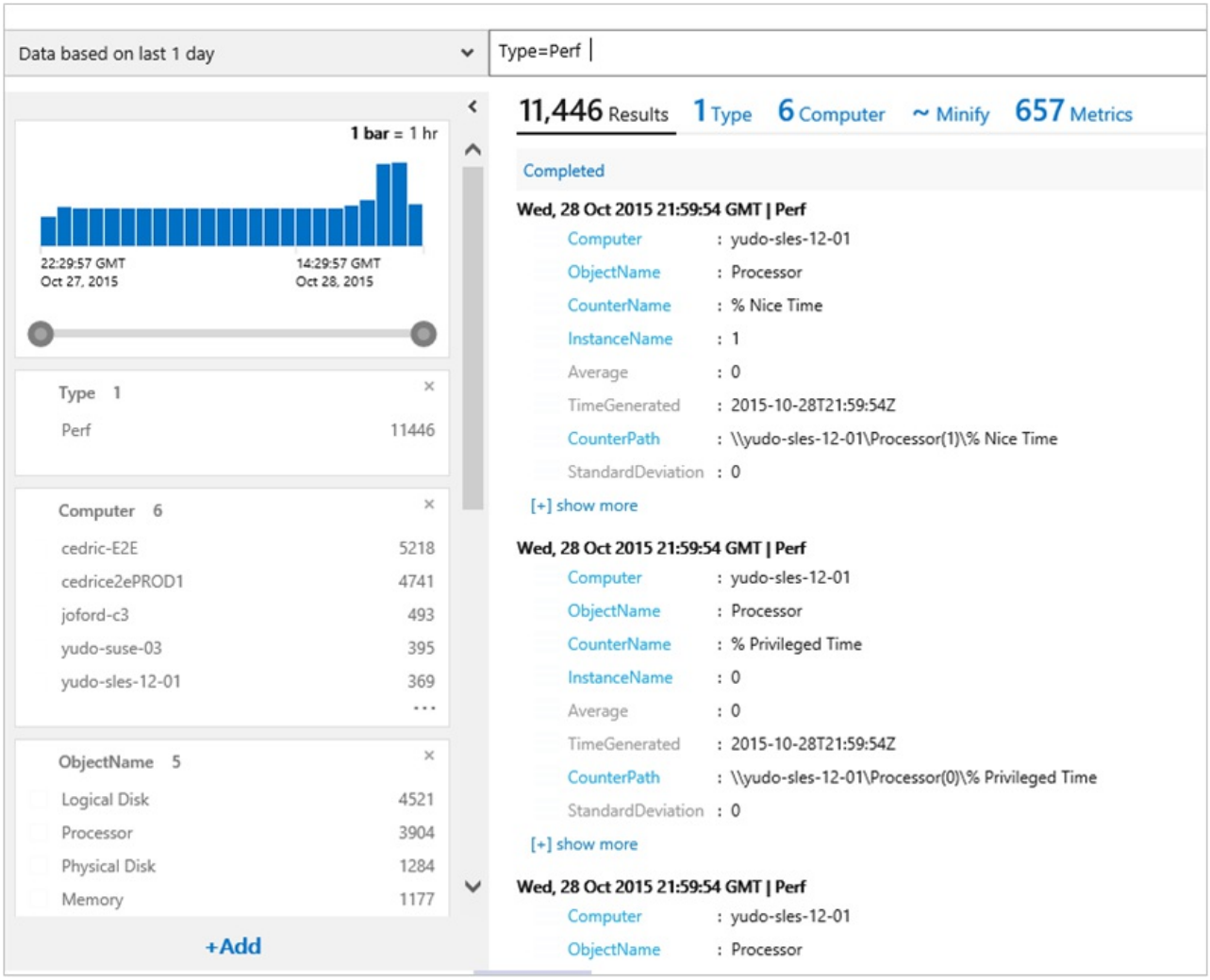


Note the name of the container next to **Name**, and search for those logs. In this example, it is `Type=ContainerLog adoring_meitner`.

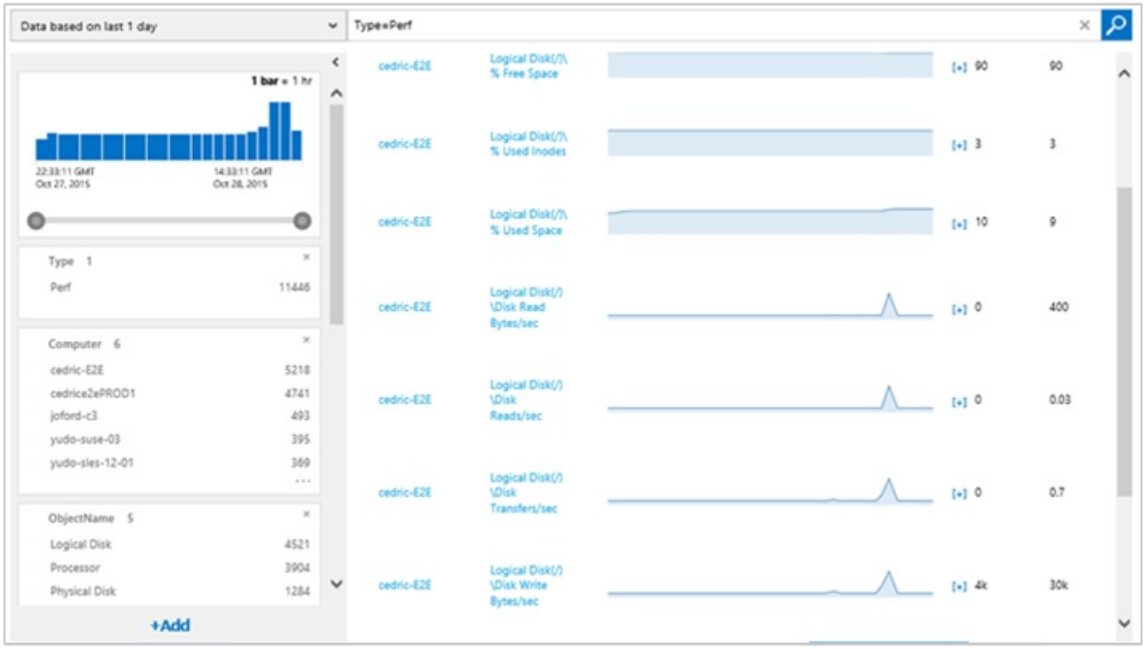
View performance information

When you're beginning to construct queries, it can help to see what's possible first. For example, to see all performance data, try a broad query by typing the following search query.

```
Type=Perf
```



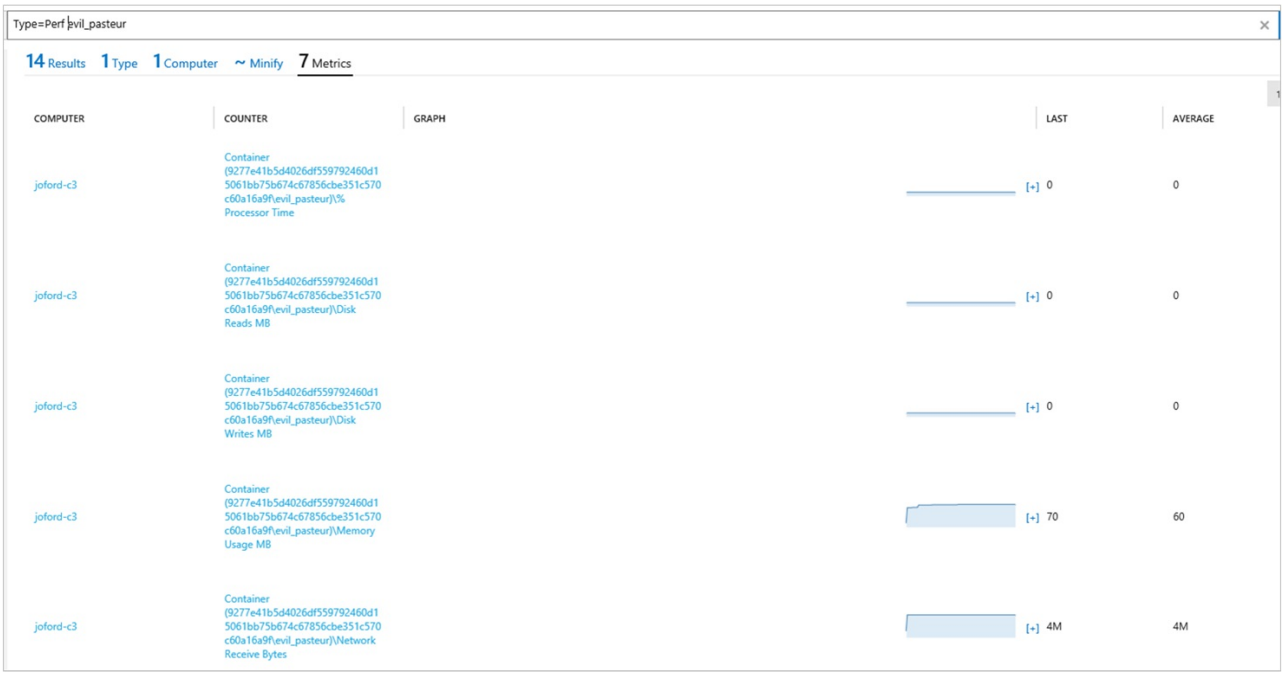
You can see this in a more graphical form when you click the word **Metrics** in the results.



You can scope the performance data you're seeing to a specific container by typing the name of it to the right of your query.

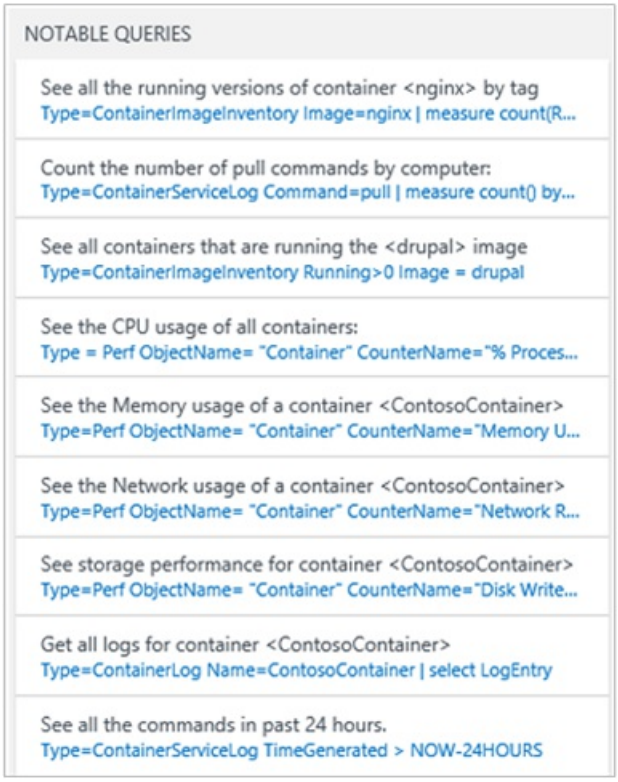
```
Type=Perf <containerName>
```

That shows the list of performance metrics that are collected for an individual container.



Example log search queries

It's often useful to build queries starting with an example or two and then modifying them to fit your environment. As a starting point, you can experiment with the **Notable Queries** blade to help you build more advanced queries.



Saving log search queries

Saving queries is a standard feature in Log Analytics. By saving them, you'll have those that you've found useful handy for future use.

After you create a query that you find useful, save it by clicking **Favorites** at the top of the Log Search page. Then you can easily access it later from the **My Dashboard** page.

Next steps

- Search logs to view detailed container data records.

Azure Key Vault Analytics solution in Log Analytics

3/10/2017 • 5 min to read • Edit Online

You can use the Azure Key Vault solution in Log Analytics to review Azure Key Vault AuditEvent logs.

To use the solution, you need to enable logging of Azure Key Vault diagnostics and direct the diagnostics to a Log Analytics workspace. It is not necessary to write the logs to Azure Blob storage.

> **NOTE**
> In January 2017, the supported way of sending logs from Key Vault to Log Analytics changed. If the Key Vault solution you are using shows *(deprecated)* in the title, refer to migrating from the old Key Vault solution for steps you need to follow.

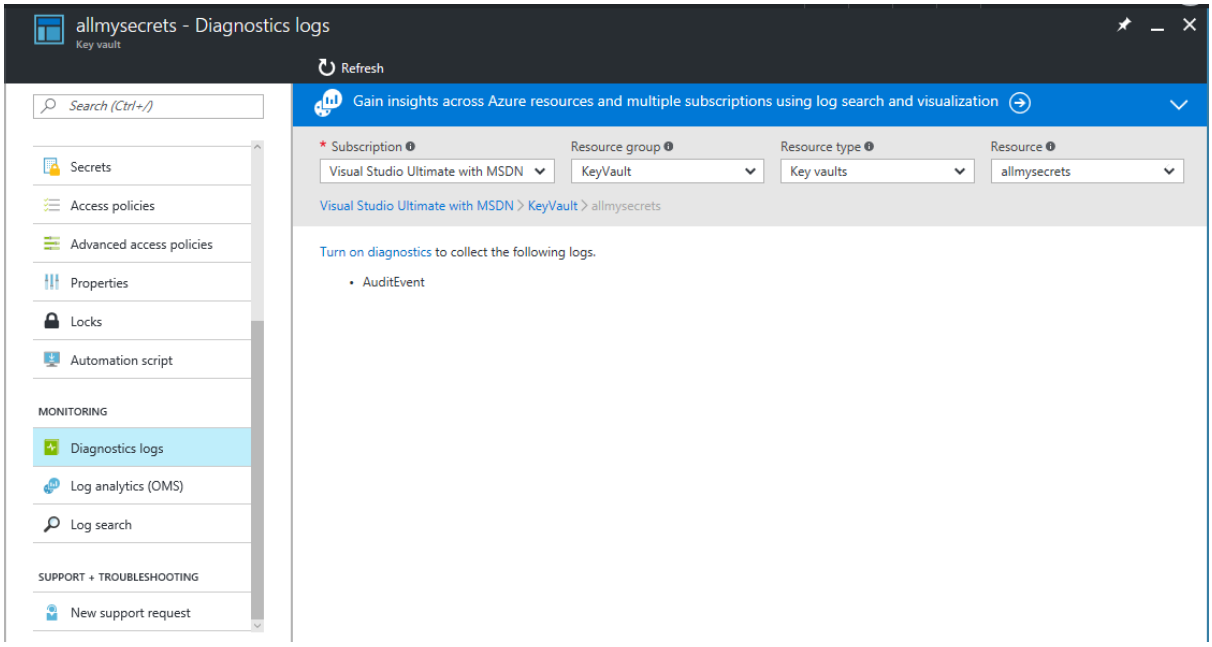
Install and configure the solution

Use the following instructions to install and configure the Azure Key Vault solution:

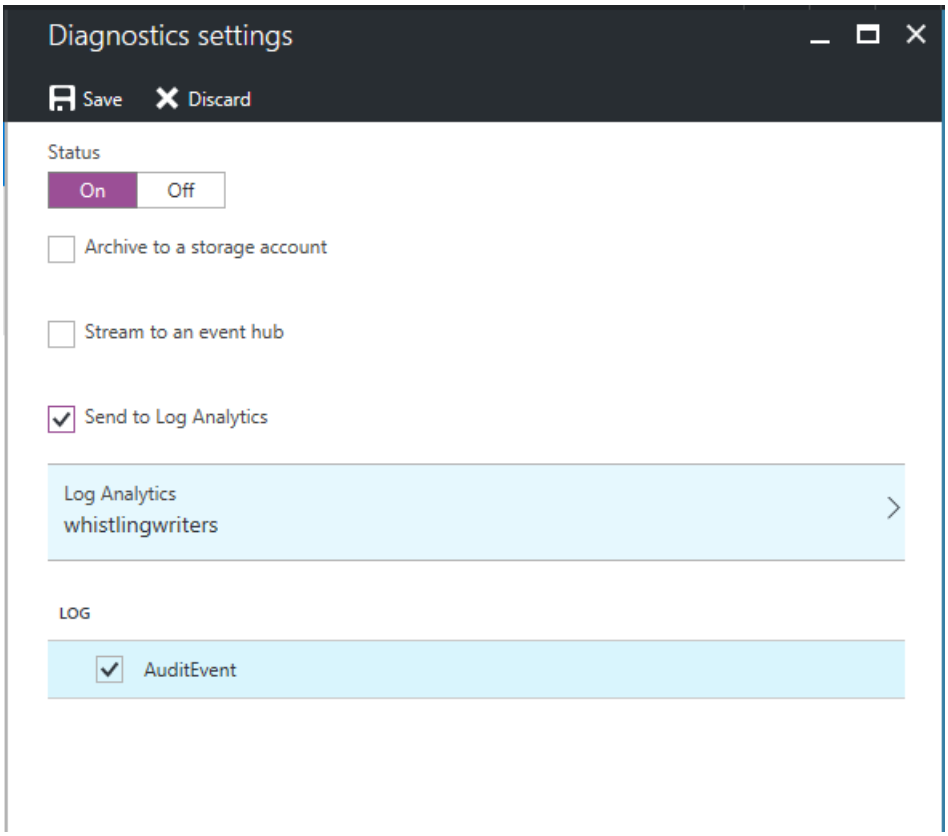
1. Enable the Azure Key Vault solution from Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery.
2. Enable diagnostics logging for the Key Vault resources to monitor, using either the portal or PowerShell

Enable Key Vault diagnostics in the portal

1. In the Azure portal, navigate to the Key Vault resource to monitor
2. Select *Diagnostics logs* to open the following page



3. Click *Turn on diagnostics* to open the following page



4. To turn on diagnostics, click *On* under *Status*
5. Click the checkbox for *Send to Log Analytics*
6. Select an existing Log Analytics workspace, or create a workspace
7. To enable *AuditEvent* logs, click the checkbox under Log
8. Click *Save* to enable the logging of diagnostics to Log Analytics

Enable Key Vault diagnostics using PowerShell

The following PowerShell script provides an example of how to use `Set-AzureRmDiagnosticSetting` to enable diagnostic logging for Key Vault:

```
$workspaceId = "/subscriptions/d2e37fee-1234-40b2-5678-0b2199de3b50/resourcegroups/oi-default-east-us/providers/microsoft.operationalinsights/workspaces/rollingbaskets"

$kv = Get-AzureRmKeyVault -VaultName 'ContosoKeyVault'

Set-AzureRmDiagnosticSetting -ResourceId $kv.ResourceId  -WorkspaceId $workspaceId -Enabled $true
```

Review Azure Key Vault data collection details

Azure Key Vault solution collects diagnostics logs directly from the Key Vault. It is not necessary to write the logs to Azure Blob storage and no agent is required for data collection.

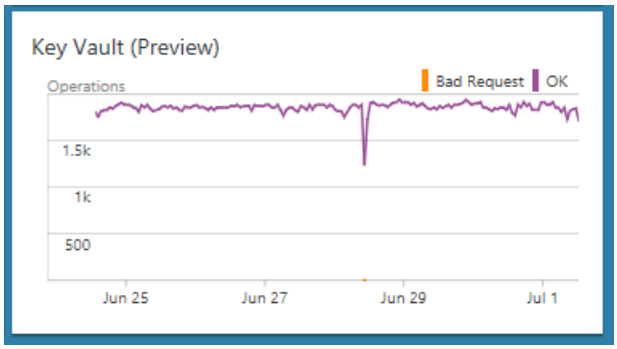
The following table shows data collection methods and other details about how data is collected for Azure Key Vault.

PLATFORM	DIRECT AGENT	SYSTEMS CENTER OPERATIONS MANAGER AGENT	AZURE	OPERATIONS MANAGER REQUIRED?	OPERATIONS MANAGER AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY

PLATFORM	DIRECT AGENT	SYSTEMS CENTER OPERATIONS MANAGER AGENT	AZURE	OPERATIONS MANAGER REQUIRED?	OPERATIONS MANAGER AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Azure	✗	✗	●	✗	✗	on arrival

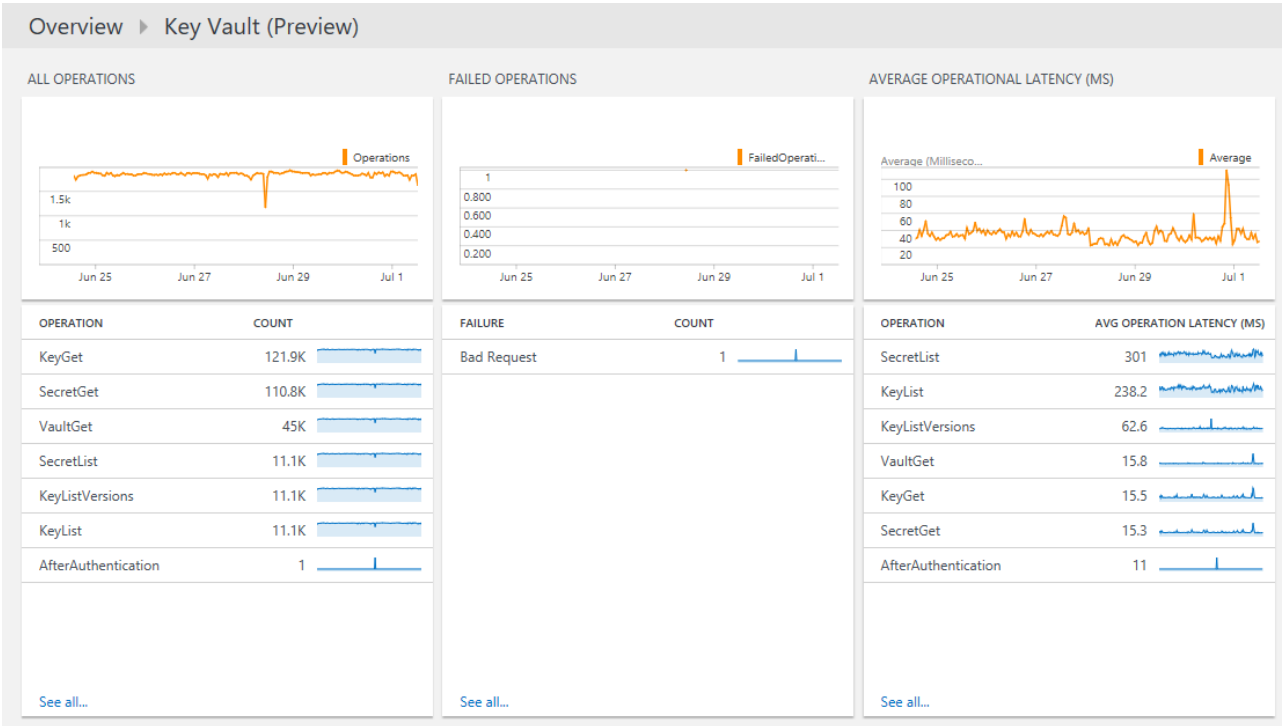
Use Azure Key Vault

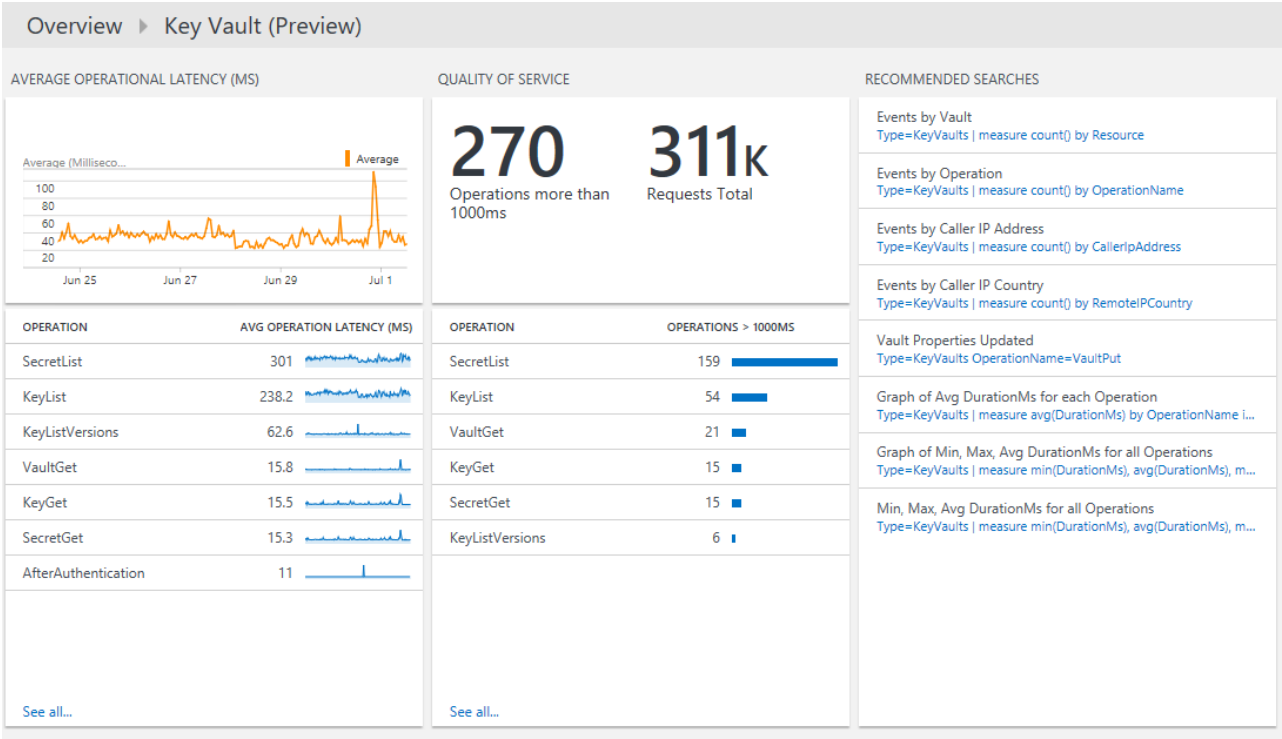
After you install the solution, view the Key Vault data by clicking the **Azure Key Vault** tile from the **Overview** page of Log Analytics.



After you click the **Overview** tile, you can view summaries of your logs and then drill in to details for the following categories:

- Volume of all key vault operations over time
- Failed operation volumes over time
- Average operational latency by operation
- Quality of service for operations with the number of operations that take more than 1000 ms and a list of operations that take more than 1000 ms





To view details for any operation

1. On the **Overview** page, click the **Azure Key Vault** tile.
2. On the **Azure Key Vault** dashboard, review the summary information in one of the blades, and then click one to view detailed information about it in the log search page.

   On any of the log search pages, you can view results by time, detailed results, and your log search history. You can also filter by facets to narrow the results.

Log Analytics records

The Azure Key Vault solution analyzes records that have a type of **KeyVaults** that are collected from AuditEvent logs in Azure Diagnostics. Properties for these records are in the following table:

PROPERTY	DESCRIPTION
Type	*AzureDiagnostics*
SourceSystem	*Azure*
CallerIpAddress	IP address of the client who made the request
Category	*AuditEvent*
CorrelationId	An optional GUID that the client can pass to correlate client-side logs with service-side (Key Vault) logs.
DurationMs	Time it took to service the REST API request, in milliseconds. This time does not include network latency, so the time that you measure on the client side might not match this time.
httpStatusCode_d	HTTP status code returned by the request (for example, *200*)
id_s	Unique ID of the request

PROPERTY	DESCRIPTION
identity_claim_appid_g	GUID for the application id
OperationName	Name of the operation, as documented in Azure Key Vault Logging
OperationVersion	REST API version requested by the client (for example *2015-06-01*)
requestUri_s	Uri of the request
Resource	Name of the key vault
ResourceGroup	Resource group of the key vault
ResourceId	Azure Resource Manager Resource ID. For Key Vault logs, this is the Key Vault resource ID.
ResourceProvider	*MICROSOFT.KEYVAULT*
ResourceType	*VAULTS*
ResultSignature	HTTP status (for example, *OK*)
ResultType	Result of REST API request (for example, *Success*)
SubscriptionId	Azure subscription ID of the subscription containing the Key Vault

Migrating from the old Key Vault solution

In January 2017, the supported way of sending logs from Key Vault to Log Analytics changed. These changes provide the following advantages:

- Logs are written directly to Log Analytics without the need to use a storage account
- Less latency from the time when logs are generated to them being available in Log Analytics
- Fewer configuration steps
- A common format for all types of Azure diagnostics

To use the updated solution:

1. Configure diagnostics to be sent directly to Log Analytics from Key Vault
2. Enable the Azure Key Vault solution by using the process described in Add Log Analytics solutions from the Solutions Gallery
3. Update any saved queries, dashboards, or alerts to use the new data type
   - Type is change from: KeyVaults to AzureDiagnostics. You can use the ResourceType to filter to Key Vault Logs.
   - Instead of: `Type=KeyVaults`, use `Type=AzureDiagnostics ResourceType=VAULTS`
   - Fields: (Field names are case-sensitive)
   - For any field that has a suffix of _s, _d, or _g in the name, change the first character to lower case
   - For any field that has a suffix of _o in name, the data is split into individual fields based on the nested field names. For example, the UPN of the caller is stored in a field

```
identity_claim_http_schemas_xmlsoap_org_ws_2005_05_identity_claims_upn_s
```

- Field CallerIpAddress changed to CallerIPAddress
- Field RemoteIPCountry is no longer present

4. Remove the *Key Vault Analytics (Deprecated)* solution. If you are using PowerShell, use

```
Set-AzureOperationalInsightsIntelligencePack -ResourceGroupName <resource group that the workspace is in> -
WorkspaceName <name of the log analytics workspace> -IntelligencePackName "KeyVault" -Enabled $false
```

Data collected before the change is not visible in the new solution. You can continue to query for this data using the old Type and field names.

Troubleshooting

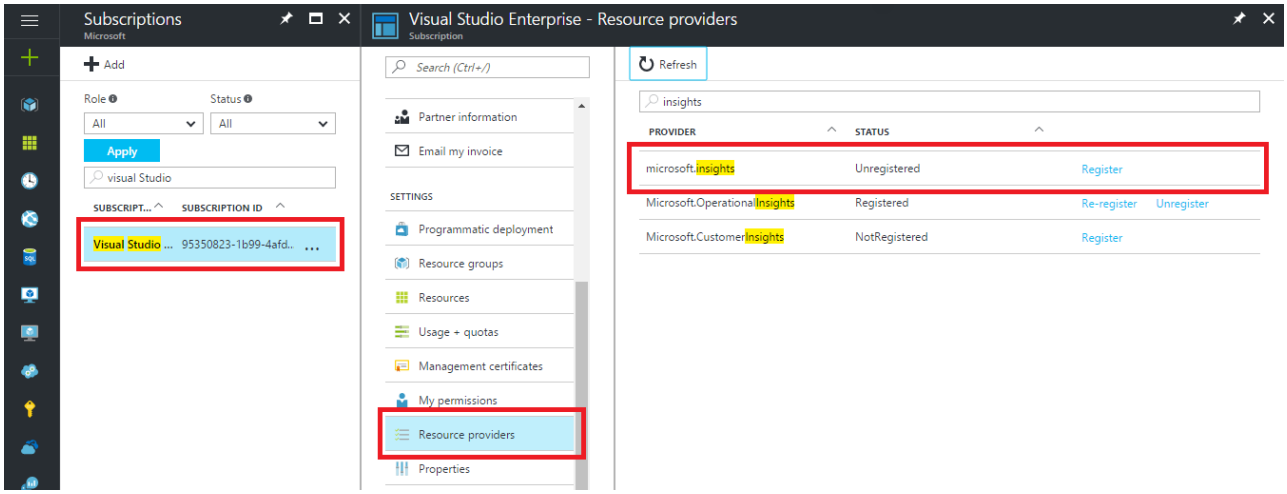
Troubleshoot Azure Diagnostics

If you receive the following error message, the Microsoft.insights resource provider is not registered:

```
Failed to update diagnostics for 'resource'. {"code":"Forbidden","message":"Please register the subscription
'subscription id' with Microsoft.Insights."}
```

To register the resource provider, perform the following steps in the Azure portal:

1. In the navigation pane on the left, click *Subscriptions*
2. Select the subscription identified in the error message
3. Click *Resource Providers*
4. Find the *Microsoft.insights* provider
5. Click the *Register* link



Once the *Microsoft.insights* resource provider is registered, retry configuring diagnostics.

In PowerShell, if you receive the following error message, you need to update your version of PowerShell:

```
Set-AzureRmDiagnosticSetting : A parameter cannot be found that matches parameter name 'WorkspaceId'.
```

Update your version of PowerShell to the November 2016 (v2.3.0), or later, release using the instructions in the Get started with Azure PowerShell cmdlets article.

Next steps

- Use Log searches in Log Analytics to view detailed Azure Key Vault data.

Network Performance Monitor solution in Log Analytics

4/12/2017 • 23 min to read • Edit Online

This document describes how to set-up and use the Network Performance Monitor solution in Log Analytics, which helps you monitor the performance of your networks-in near real-time-to detect and locate network performance bottlenecks. With the Network Performance Monitor solution, you can monitor the loss and latency between two networks, subnets or servers. Network Performance Monitor detects network issues like traffic blackholing, routing errors, and issues that conventional network monitoring methods are not able to detect. Network Performance Monitor generates alerts and notifies as and when a threshold is breached for a network link. These thresholds can be learned automatically by the system or you can configure them to use custom alert rules. Network Performance Monitor ensures timely detection of network performance issues and localizes the source of the problem to a particular network segment or device.

You can detect network issues with the solution dashboard which displays summarized information about your network including recent network health events, unhealthy network links, and subnetwork links that are facing high packet loss and latency. You can drill-down into a network link to view the current health status of subnetwork links as well as node-to-node links. You can also view the historical trend of loss and latency at the network, subnetwork, and node-to-node level. You can detect transient network issues by viewing historical trend charts for packet loss and latency and locate network bottlenecks on a topology map. The interactive topology graph allows you to visualize the hop-by-hop network routes and determine the source of the problem. Like any other solutions, you can use Log Search for various analytics requirements to create custom reports based on the data collected by Network Performance Monitor.

The solution uses synthetic transactions as a primary mechanism to detect network faults. So, you can use it without regard for a specific network device's vendor or model. It works across on-premises, cloud (IaaS), and hybrid environments. The solution automatically discovers the network topology and various routes in your network.

Typical network monitoring products focus on monitoring the network device (routers, switches etc.) health but do not provide insights into the actual quality of network connectivity between two points, which Network Performance Monitor does.

Using the solution standalone

If you want to monitor the quality of network connections between their critical workloads, networks, datacenters or office sites, then you can use the Network Performance Monitor solution by itself to monitor connectivity health between:

- multiple datacenters or office sites that are connected using a public or private network
- critical workloads that are running line of business applications
- public cloud services like Microsoft Azure or Amazon Web Services (AWS) and on-premises networks, if you have IaaS (VM) available and you have gateways configured to allow communication between on-premises networks and cloud networks
- Azure and on-premises networks when you use Express Route

Using the solution with other networking tools

If you want to monitor a line of business application, you can use the Network Performance Monitor solution as a companion solution to other network tools. A slow network can lead to slow applications and Network Performance Monitor can help you investigate application performance issues that are caused by underlying networking issues. Because the solution does not require any access to network devices, the application administrator doesn't need to

rely on a networking team to provide information about how the network is affecting applications.

Also, if you already invest in other network monitoring tools, then the solution can complement those tools because most traditional network monitoring solutions do not provide insights into end-to-end network performance metrics like loss and latency. The Network Performance Monitor solution can help fill that gap.

Installing and configuring agents for the solution

Use the basic processes to install agents at Connect Windows computers to Log Analytics and Connect Operations Manager to Log Analytics.

> **NOTE**
> You'll need to install at least 2 agents in order to have enough data to discover and monitor your network resources. Otherwise, the solution will remain in a configuring state until you install and configure additional agents.

Where to install the agents

Before you install agents, consider the topology of your network and what parts of the network you want to monitor. We recommend that you install more than one agent for each subnet that you want to monitor. In other words, for every subnet that you want to monitor, choose two or more servers or VMs and install the agent on them.

If you are unsure about the topology of your network, install the agents on servers with critical workloads where you want to monitor the network performance. For example, you might want to keep track of a network connection between a Web server and a server running SQL Server. In this example, you'd install an agent on both servers.

Agents monitor network connectivity (links) between hosts -- not the hosts themselves. So, to monitor a network link, you must install agents on both endpoints of that link.

Configure agents

If you intend to use the ICMP protocol for synthetic transactions, you need to enable the following firewall rules for reliably utilizing ICMP:

```
netsh advfirewall firewall add rule name="NPMDICMPV4Echo" protocol="icmpv4:8,any" dir=in action=allow
netsh advfirewall firewall add rule name="NPMDICMPV6Echo" protocol="icmpv6:128,any" dir=in action=allow
netsh advfirewall firewall add rule name="NPMDICMPV4DestinationUnreachable" protocol="icmpv4:3,any" dir=in
action=allow
netsh advfirewall firewall add rule name="NPMDICMPV6DestinationUnreachable" protocol="icmpv6:1,any" dir=in
action=allow
netsh advfirewall firewall add rule name="NPMDICMPV4TimeExceeded" protocol="icmpv4:11,any" dir=in action=allow
netsh advfirewall firewall add rule name="NPMDICMPV6TimeExceeded" protocol="icmpv6:3,any" dir=in action=allow
```

If you intend to use the TCP protocol you need to open firewall ports for those computers to ensure that agents can communicate. You need to download and then run the EnableRules.ps1 PowerShell script without any parameters in a PowerShell window with administrative privileges.

The script creates registry keys required by the Network Performance Monitor and it creates Windows firewall rules to allow agents to create TCP connections with each other. The registry keys created by the script also specify whether to log the debug logs and the path for the logs file. It also defines the agent TCP port used for communication. The values for these keys are automatically set by the script, so you should not manually change these keys.

The port opened by default is 8084. You can use a custom port by providing the parameter `portNumber` to the script. However, the same port should be used on all the computers where the script is run.

> **NOTE**
>
> The EnableRules.ps1 script configures Windows firewall rules only on the computer where the script is run. If you have a network firewall, you should make sure that it allows traffic destined for the TCP port being used by Network Performance Monitor.

Configuring the solution

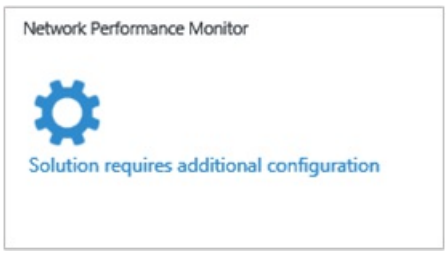
Use the following information to install and configure the solution.

1. The Network Performance Monitor solution acquires data from computers running Windows Server 2008 SP 1 or later or Windows 7 SP1 or later, which are the same requirements as the Microsoft Monitoring Agent (MMA). NPM agents can also run on Windows desktop/client operating systems (Windows 10, Windows 8.1, Windows 8 and Windows 7).

   > **NOTE**
   >
   > The agents for Windows server operating systems support both TCP and ICMP as the protocols for synthetic transaction. However, the agents for Windows client operating systems only support ICMP as the protocol for synthetic transaction.

2. Add the Network Performance Monitor solution to your workspace from Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery.

3. In the OMS portal, you'll see a new tile titled **Network Performance Monitor** with the message *Solution requires additional configuration*. You'll need to configure the solution to add networks based on subnetworks and nodes that are discovered by agents. Click **Network Performance Monitor** to start configuring the default network.



Configure the solution with a default network

On the configuration page, you'll see a single network named **Default**. When you haven't defined any networks, all the automatically-discovered subnets are placed in the Default network.

Whenever you create a network, you add a subnet to it and that subnet is removed from the Default network. If you delete a network, all its subnets are automatically returned to the Default network.

In other words, the Default network is the container for all the subnets that are not contained in any user-defined network. You cannot edit or delete the Default network. It always remains in the system. However, you can create as many networks as you need.

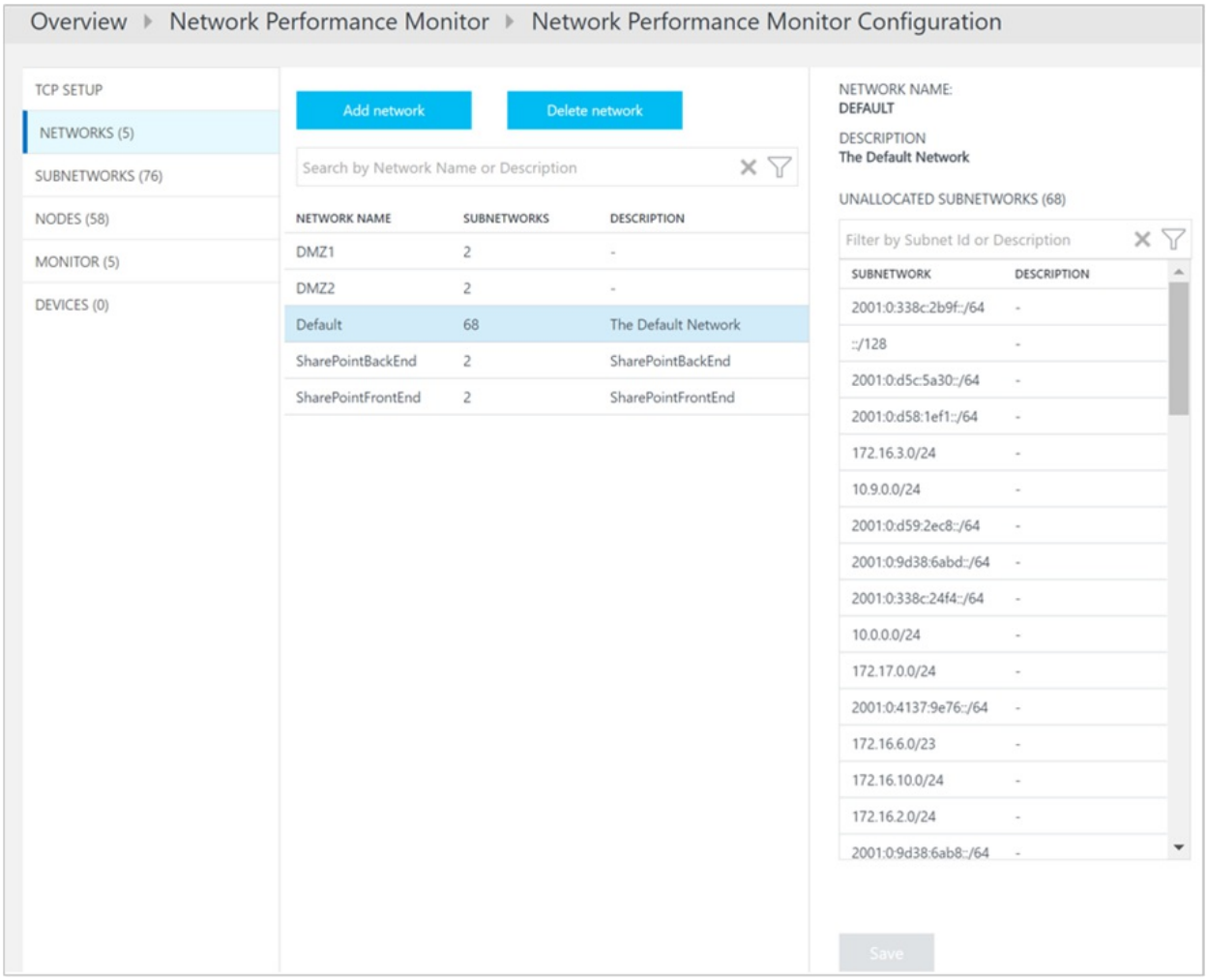
In most cases, the subnets in your organization will be arranged in more than one network and you should create one or more networks to logically group your subnets.

Create new networks

A network in Network Performance Monitor is a container for subnets. You can create a network with any name that you want and add subnets to the network. For example, you can create a network named *Building 1* and then add subnets, or you can create a network named *DMZ* and then add all subnets belonging to demilitarized zone to this network.

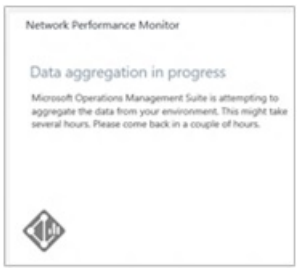
To create a new network

1. Click **Add network** and then type the network name and description.
2. Select one or more subnets, and then click **Add**.
3. Click **Save** to save the configuration.

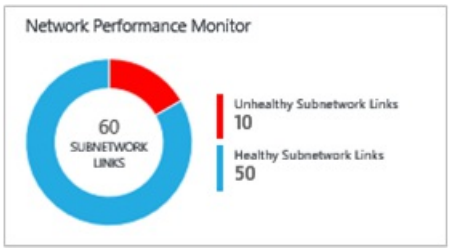


Wait for data aggregation

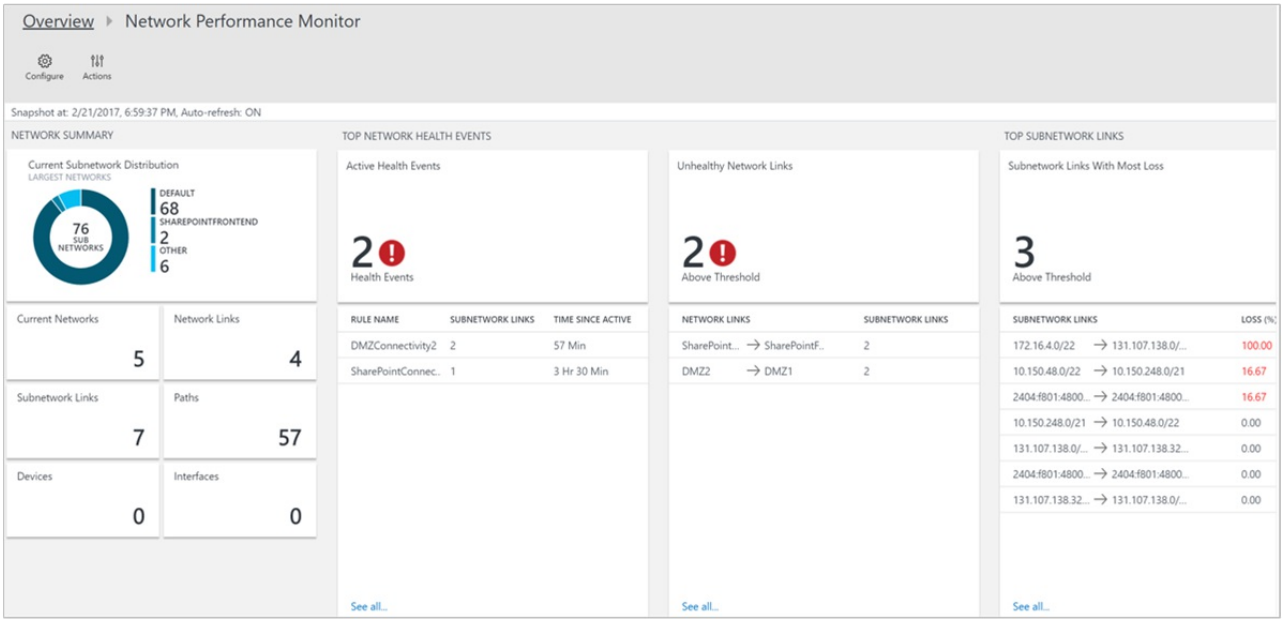
After you've saved the configuration for first time, the solution starts collecting network packet loss and latency information between the nodes where agents are installed. This process can take a while, sometimes over 30 minutes. During this state, the Network Performance Monitor tile in the overview page displays a message stating *Data aggregation in process*.



When the data has been uploaded, you'll see the Network Performance Monitor tile updated showing data.



Click the tile to view the Network Performance Monitor dashboard.

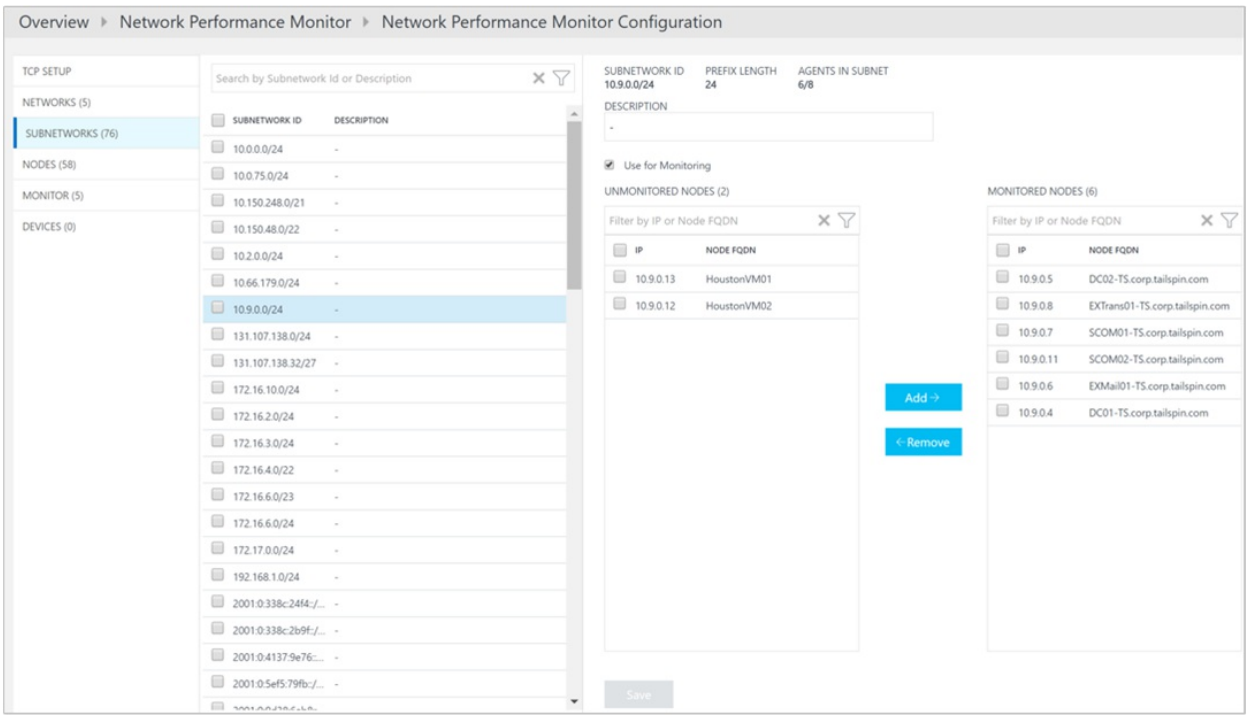


Edit monitoring settings for subnets

All subnets where at least one agent was installed are listed on the **Subnetworks** tab in the configuration page.

To enable or disable monitoring for particular subnetworks

1. Select or clear the box next to the **subnetwork ID** and then ensure that **Use for Monitoring** is selected or cleared, as appropriate. You can select or clear multiple subnets. When disabled, subnetworks are not monitored as the agents will be updated to stop pinging other agents.
2. Choose the nodes that you want to monitor for a particular subnetwork by selecting the subnetwork from the list and moving the required nodes between the lists containing unmonitored and monitored nodes. You can add a custom **description** to the subnetwork, if you like.
3. Click **Save** to save the configuration.

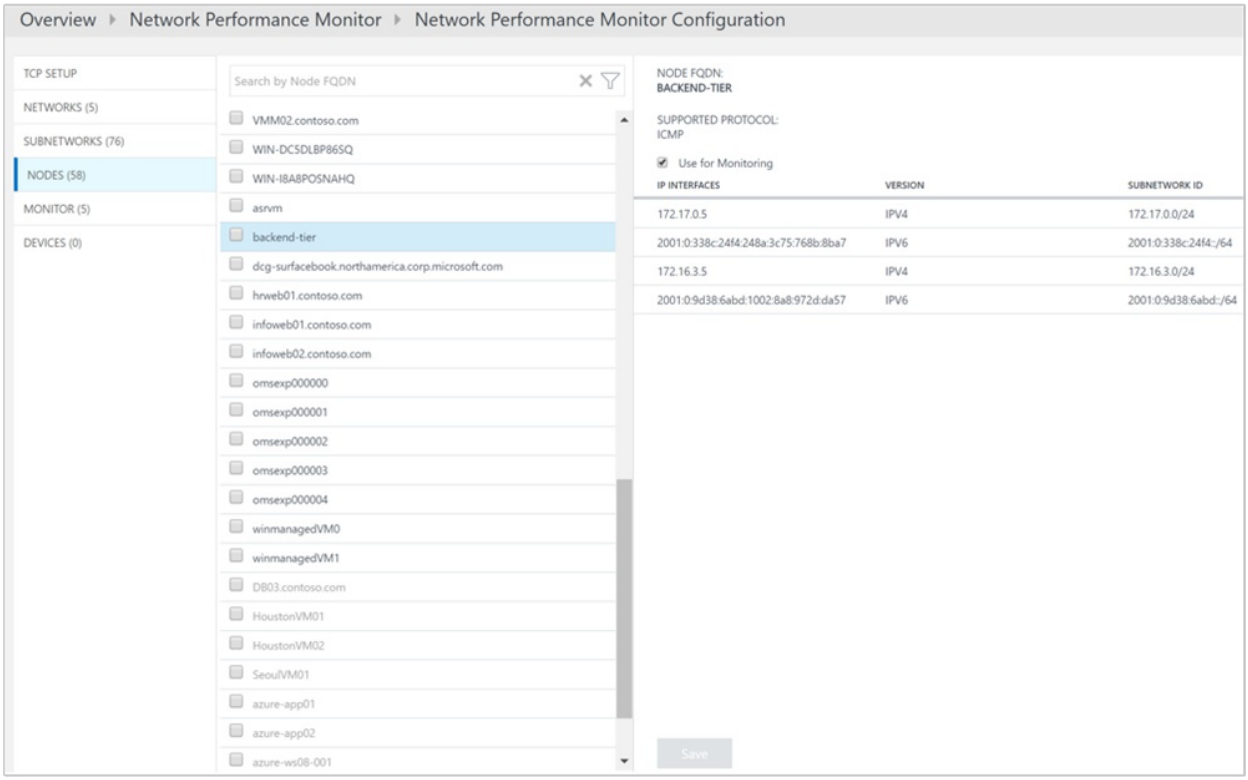


Choose nodes to monitor

All the nodes that have an agent installed on them are listed in the **Nodes** tab.

To enable or disable monitoring for nodes

1. Select or clear the nodes that you want to monitor or stop monitoring.
2. Click **Use for Monitoring**, or clear it, as appropriate.
3. Click **Save**.



Set monitoring rules

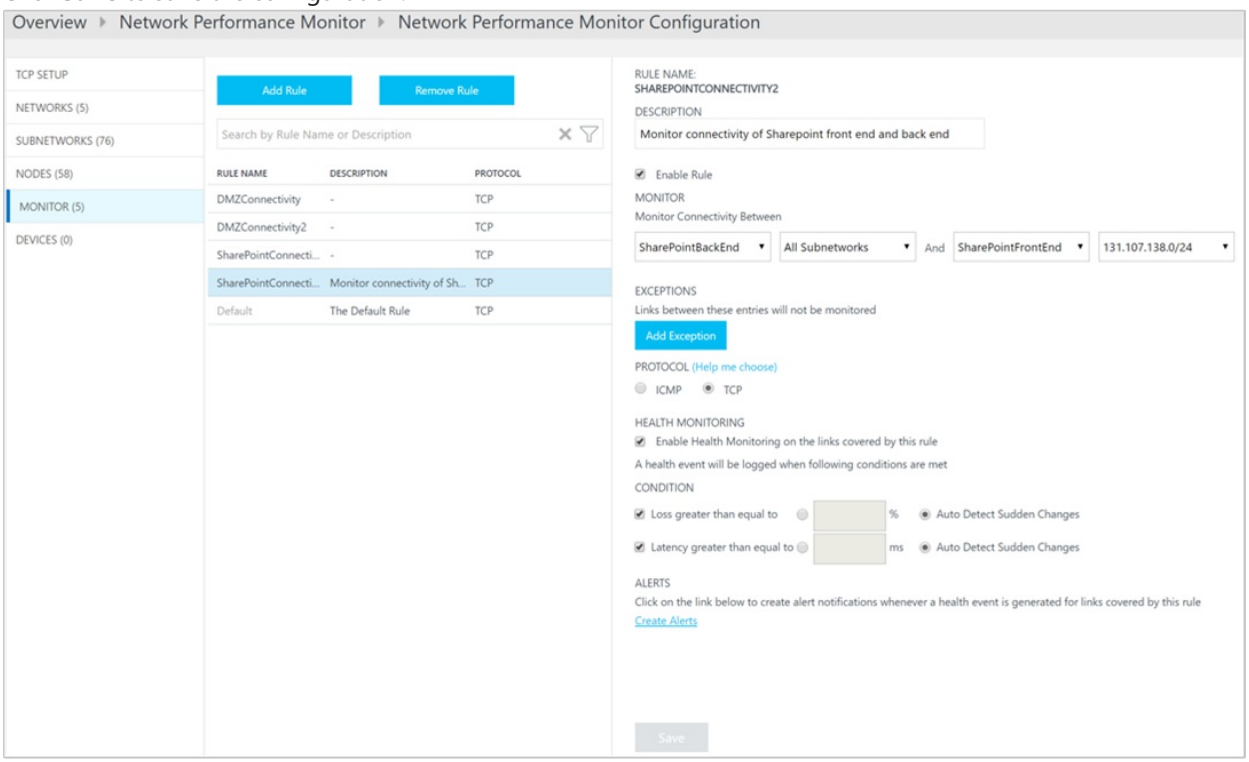
Network Performance Monitor generates health events about the connectivity between a pair of nodes or subnetwork or network links when a threshold is breached. These thresholds can be learned automatically by the system or you can configure them custom alert rules.

The *Default rule* is created by the system and it creates a health event whenever loss or latency between any pair of networks or subnetwork links breaches the system-learned threshold. You can choose to disable the default rule

and create custom monitoring rules

To create custom monitoring rules

1. Click **Add Rule** in the **Monitor** tab and enter the rule name and description.
2. Select the pair of network or subnetwork links to monitor from the lists.
3. First select the network in which the first subnetwork/s of interest is contained from the network dropdown, and then select the subnetwork/s from the corresponding subnetwork dropdown. Select **All subnetworks** if you want to monitor all the subnetworks in a network link. Similarly select the other subnetwork/s of interest. And, you can click **Add Exception** to exclude monitoring for particular subnetwork links from the selection you've made.
4. Choose between ICMP and TCP protocols for executing synthetic transactions.
5. If you don't want to create health events for the items you've selected, then clear **Enable health monitoring on the links covered by this rule**.
6. Choose monitoring conditions. You can set custom thresholds for health event generation by typing threshold values. Whenever the value of the condition goes above its selected threshold for the selected network/subnetwork pair, a health event is generated.
7. Click **Save** to save the configuration.



After you save a monitoring rule, you can integrate that rule with Alert Management by clicking **Create Alert**. An alert rule is automatically created with the search query and other required parameters automatically filled-in. Using an alert rule, you can receive email-based alerts, in addition to the existing alerts within NPM. Alerts can also trigger remedial actions with runbooks or they can integrate with existing service management solutions using webhooks. You can click **Manage Alert** to edit the alert settings.

Choose the right protocol-ICMP or TCP

Network Performance Monitor (NPM) uses synthetic transactions to calculate network performance metrics like packet loss and link latency. To understand this better, consider an NPM agent connected to one end of a network link. This NPM agent sends probe packets to a second NPM agent connected to another end of the network. The second agent replies with response packets. This process is repeated a few times. By measuring the number of replies and time taken to receive each reply, the first NPM agent assesses link latency and packet drops.

The format, size and sequence of these packets is determined by the protocol that you choose when you create monitoring rules. Based on protocol of the packets, the intermediate network devices (routers, switches etc.) might process these packets differently. Consequently, your protocol choice affects the accuracy of the results. And, your

protocol choice also determines whether you must take any manual steps after you deploy the NPM solution.

NPM offers you the choice between ICMP and TCP protocols for executing synthetic transactions. If you choose ICMP when you create a synthetic transaction rule, the NPM agents use ICMP ECHO messages to calculate the network latency and packet loss. ICMP ECHO uses the same message that is sent by the conventional Ping utility. When you use TCP as the protocol, NPM agents send TCP SYN packet over the network. This is followed by a TCP handshake completion and then removing the connection using RST packets.

Points to consider before choosing the protocol

Consider the following information before you choose a protocol to use:

Discovering multiple network routes

TCP provides more accurate when discovering multiple routes and it needs with fewer agents in each subnet. For example, one or two agents using TCP can discover all redundant paths between subnets. However, you need several agents using ICMP to achieve similar results. Using ICMP, if you have *N* number of routes between two subnets you need more than 5*N* agents in either a source or destination subnet.

Accuracy of results

Routers and switches tend to assign lower priority to ICMP ECHO packets compared to TCP packets. In certain situations, when network devices are heavily loaded, the data obtained by TCP more closely reflects the loss and latency experienced by applications. This occurs because most of the application traffic flows over TCP. In such cases, ICMP provides less accurate results compared to TCP.

Firewall configuration

TCP protocol requires that TCP packets are sent to a destination port. The default port used by NPM agents is 8084, however you can change this when you configure agents. So, you need to ensure that your network firewalls or NSG rules (in Azure) are allowing traffic on the port. You also need to make sure that the local firewall on the computers where agents are installed is configured to allow traffic on this port.

You can use PowerShell scripts to configure firewall rules on your computers running Windows, however you need to configure your network firewall manually.

In contrast, ICMP does not operate using port. In most enterprise scenarios, ICMP traffic is permitted through the firewalls to allow you to use network diagnostics tools like the Ping utility. So, if you can Ping one machine from another, then you can use the ICMP protocol without having to configure firewalls manually.

> **NOTE**
> In case you are not sure what protocol to use, choose ICMP to start with. If you are not satisfied with the results, you can always switch to TCP later.

How to switch the protocol

If you chose to use ICMP during deployment, you can switch to TCP at any time by editing the default monitoring rule.

To edit the default monitoring rule

1. Navigate to **Network Performance** > **Monitor** > **Configure** > **Monitor** and then click **Default rule**.
2. Scroll to the **Protocol** section and select the protocol that you want to use.
3. Click **Save** to apply the setting.

Even if the default rule is using a specific protocol, you can create new rules with a different protocol. You can even create a mix of rules where some of the rules use ICMP and another uses TCP.

Data collection details

Network Performance Monitor uses TCP SYN-SYNACK-ACK handshake packets when TCP is chosen and ICMP ECHO ICMP ECHO REPLY when ICMP is chosen as the protocol to collect loss and latency information. Traceroute is

also used to get topology information.

The following table shows data collection methods and other details about how data is collected for Network Performance Monitor.

PLATFORM	DIRECT AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows	✓	✓	✗	✗	✗	TCP handshakes/ICMP ECHO messages every 5 seconds, data sent every 3 minutes

The solution uses synthetic transactions to assess the health of the network. OMS agents installed at various point in the network exchange TCP packets or ICMP Echo (depending on the protocol selected for monitoring) with one another. In the process, agents learn the round-trip time and packet loss, if any. Periodically, each agent also performs a trace route to other agents to find all the various routes in the network that must be tested. Using this data, the agents can deduce the network latency and packet loss figures. The tests are repeated every five seconds and data is aggregated for a period of three minutes by the agents before uploading it to the Log Analytics service.

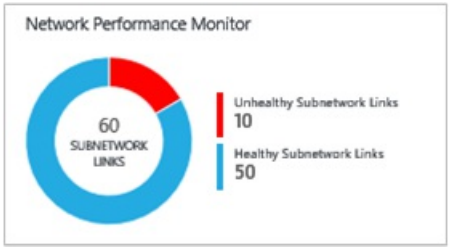
> **NOTE**
> Although agents communicate with each other frequently, they do not generate a lot of network traffic while conducting the tests. Agents rely only on TCP SYN-SYNACK-ACK handshake packets to determine the loss and latency -- no data packets are exchanged. During this process, agents communicate with each other only when needed and the agent communication topology is optimized to reduce network traffic.

Using the solution

This section explains all the dashboard functions and how to use them.

Solution Overview tile

After you've enabled the Network Performance Monitor solution, the solution tile on the OMS Overview page provides a quick overview of the network health. It displays a doughnut chart showing the number of healthy and unhealthy subnetwork links. When you click the tile, it opens the solution dashboard.



Network Performance Monitor solution dashboard

The **Network Summary** blade shows a summary of the networks along with their relative size. This is followed by tiles showing total number of network links, subnet links and paths in the system (a path consists of the IP addresses of two hosts with agents and all the hops between them).

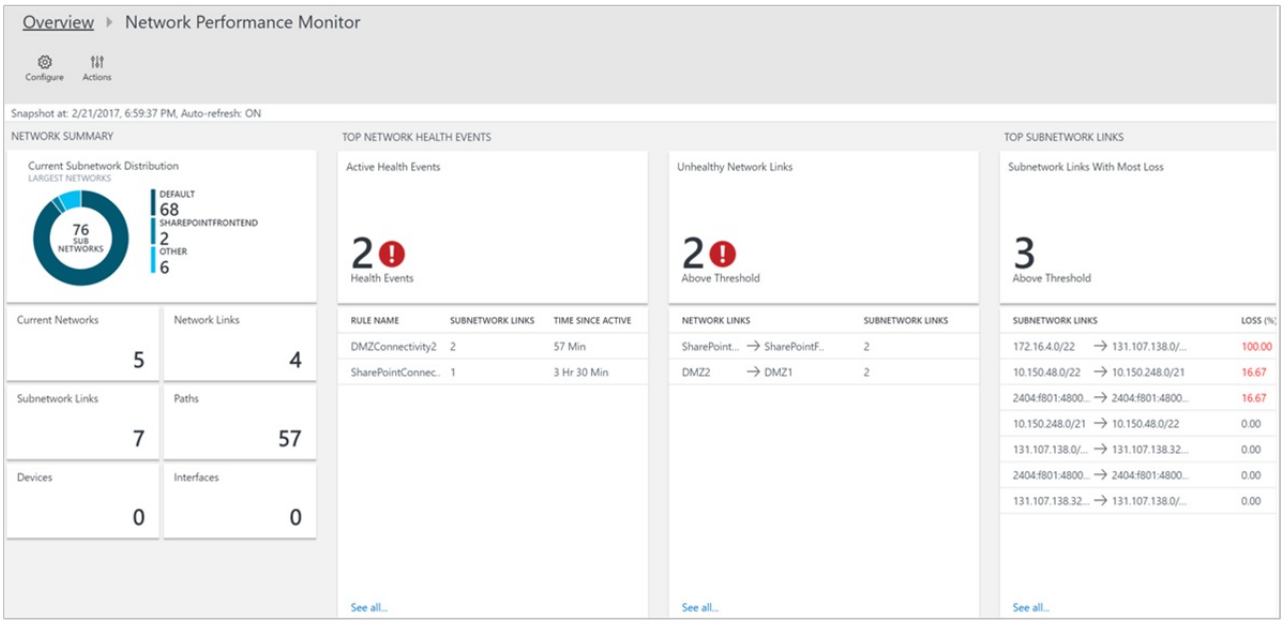
The **Top Network Health Events** blade provides a list of most recent health events and alerts in the system and the time since the event has been active. A health event or alert is generated whenever the packet loss or latency of

a network or subnetwork link exceeds a threshold.

The **Top Unhealthy Network Links** blade shows a list of unhealthy network links. These are the network links that have one or more adverse health event for them at the moment.

The **Top Subnetwork Links with Most Loss** and **Subnetwork Links with Most Latency** blades show the top subnetwork links by packet loss and top subnetwork links by latency respectively. High latency or some amount of packet loss might be expected on certain network links. Such links appear in the top ten lists but are not marked unhealthy.

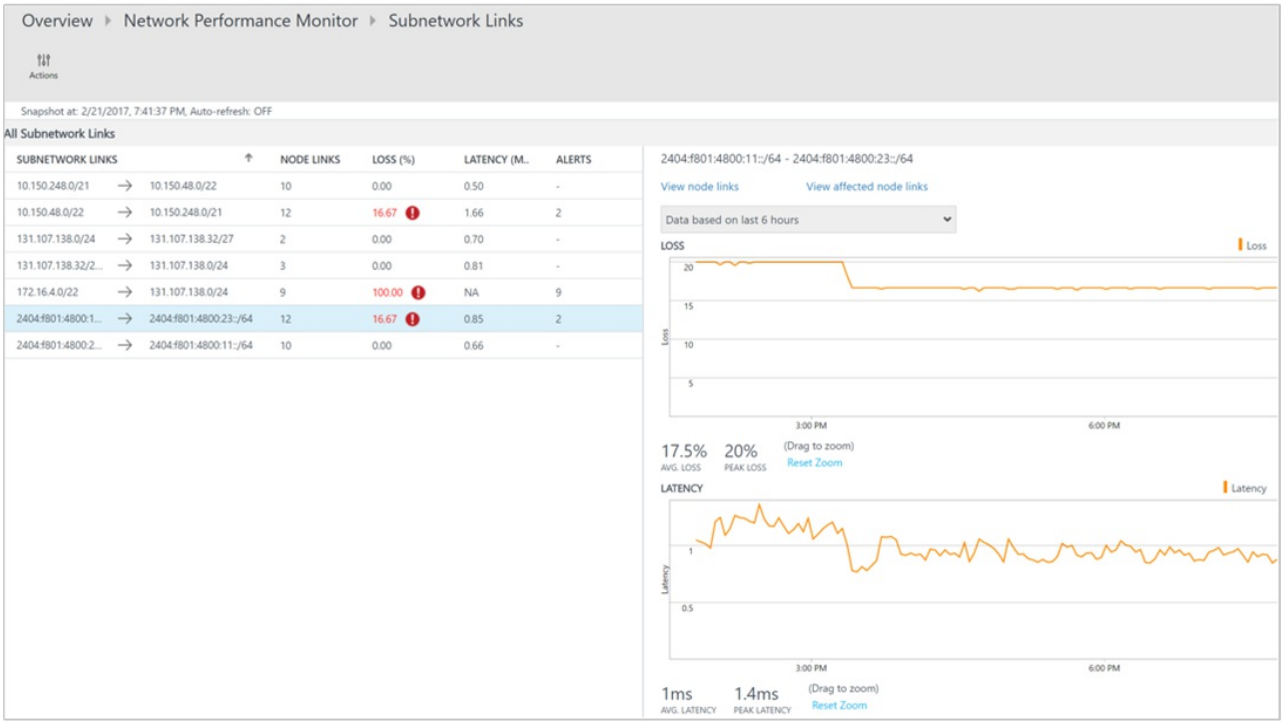
The **Common Queries** blade contains a set of search queries that fetch raw network monitoring data directly. You can use these queries as a starting point for creating your own queries for customized reporting.



Drill-down for depth

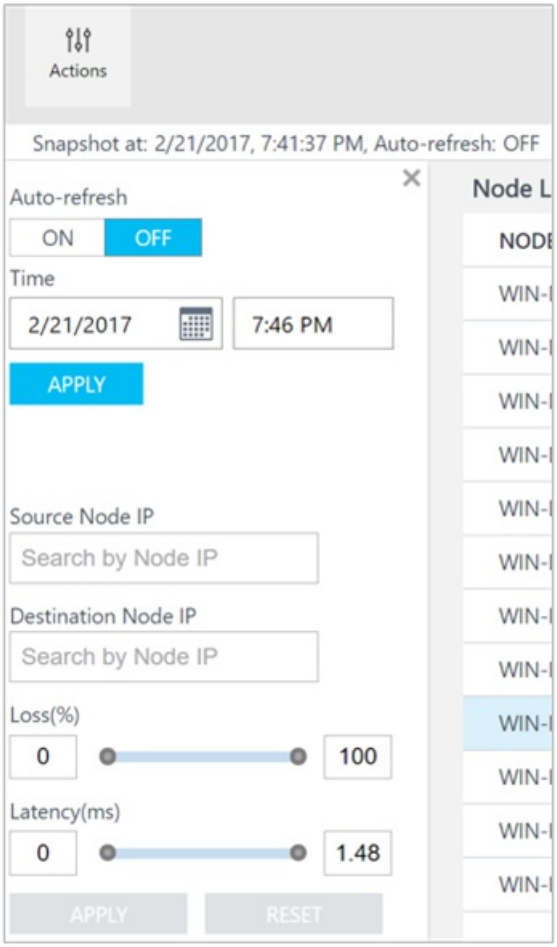
You can click various links on the solution dashboard to drill-down deeper into any area of interest. For example, when you see an alert or an unhealthy network link appear on the dashboard, you can click it to investigate further. You'll be taken to a page that lists all the subnetwork links for the particular network link. You will be able to see the loss, latency and health status of each subnetwork link and quickly find out what subnetwork links are causing the problem. You can then click **View node links** to see all the node links for the unhealthy subnet link. Then, you can see individual node-to-node links and find the unhealthy node links.

You can click **View topology** to view the hop-by-hop topology of the routes between the source and destination nodes. The unhealthy routes or hops are shown in red so that you can quickly identify the problem to a particular portion of the network.



Network State Recorder

Each view displays a snapshot of your network health at a particular point in time. By default, the most recent state is shown. The bar at the top of the page shows the point in time for which the state is being displayed. You can choose to go back in time and view the snapshot of your network health by clicking on the bar on **Actions**. You can also choose to enable or disable auto-refresh for any page while you view the latest state.



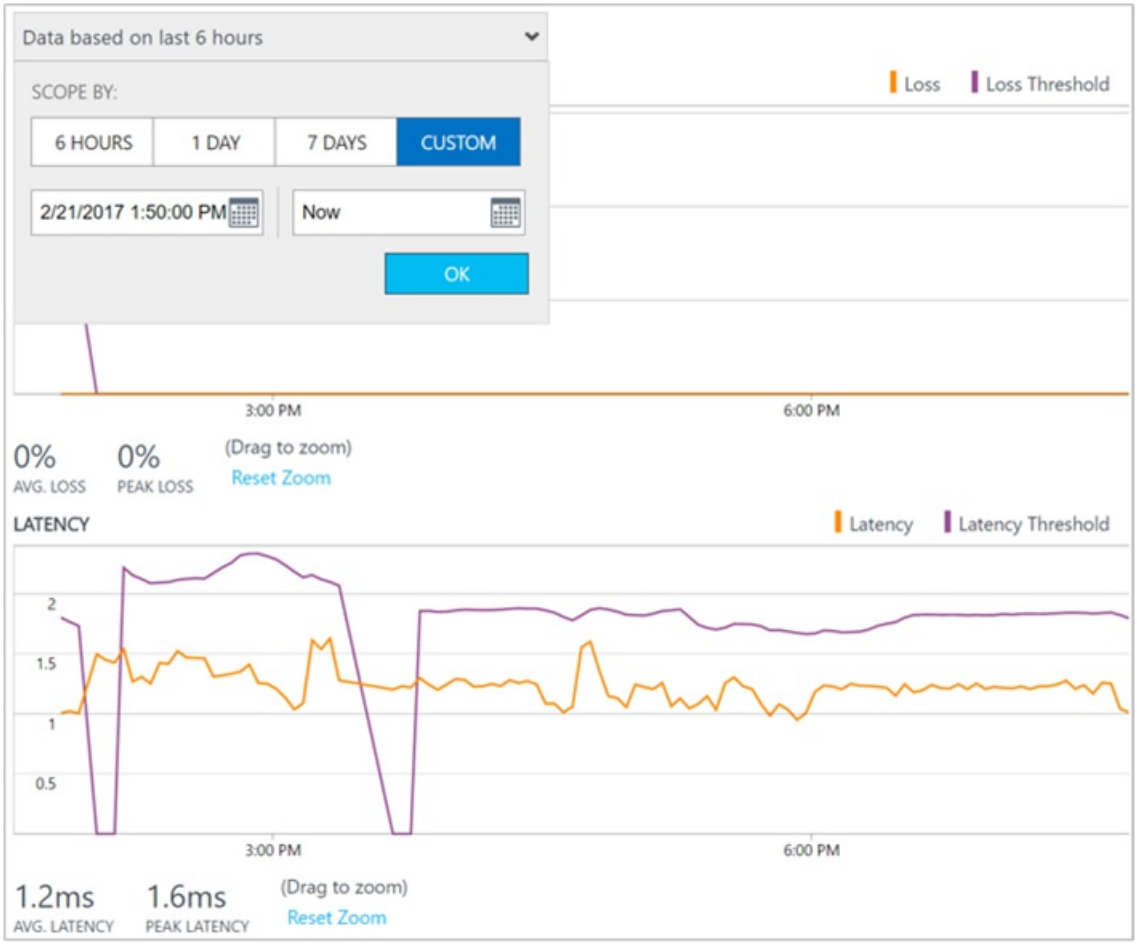
Trend charts

At each level that you drill-down, you can see the trend of loss and latency for a network link. Trend charts are also available for Subnetwork and Node links. You can change the time interval for the graph to plot by using the time

control at the top of the chart.

Trend charts show you a historical perspective of the performance of a network link. Some network issues are transient in nature and would be hard to catch only by looking at the current state of the network. This is because issues can surface quickly and disappear before anyone notices, only to reappear at a later point in time. Such transient issues can also be difficult for application administrators because those issues often surface as unexplained increases in application response time, even when all application components appear to run smoothly.

You can easily detect those kinds of issues by looking at a trend chart where the issue will appear as a sudden spike in network latency or packet loss.



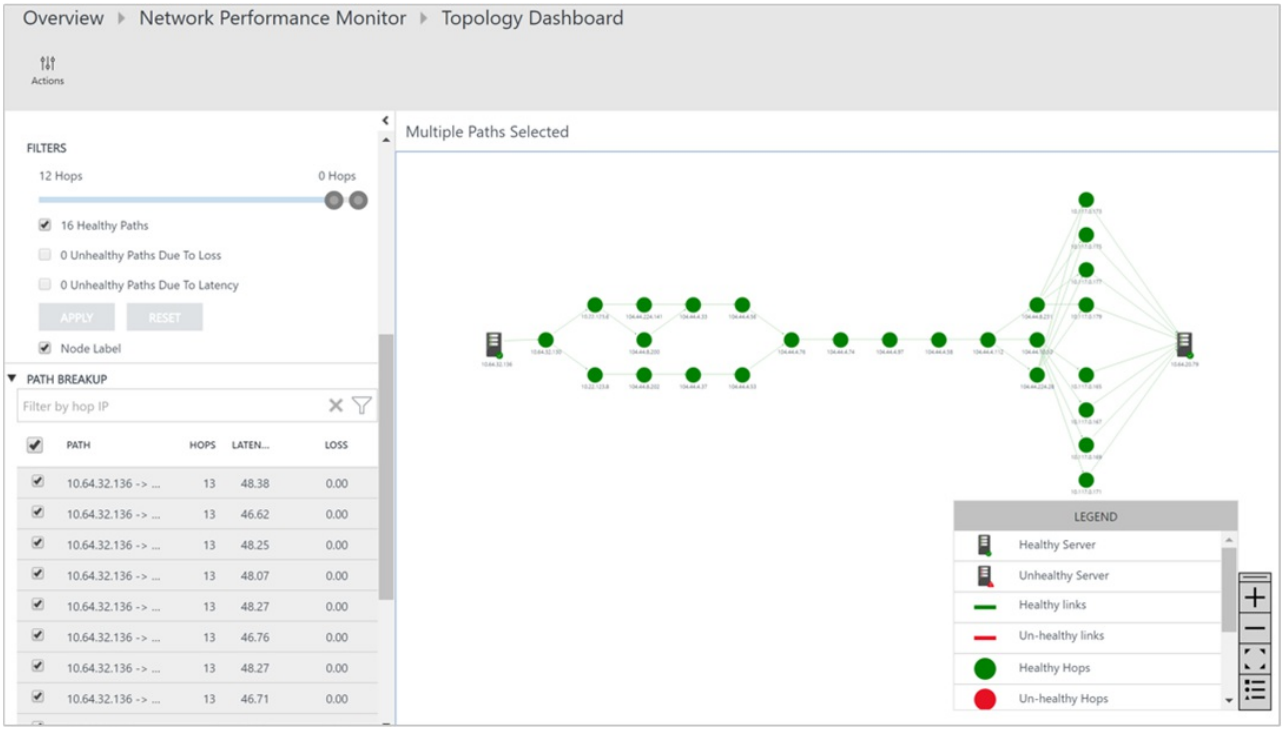
Hop-by-hop topology map

Network Performance Monitor shows you the hop-by-hop topology of routes between two nodes on an interactive topology map. You can view the topology map by selecting a node link and then clicking **View topology**. Also, you can view the topology map by clicking **Paths** tile on the dashboard. When you click **Paths** on the dashboard, you'll have to select the source and destination nodes from the left hand panel and then click **Plot** to plot the routes between the two nodes.

The topology map displays how many routes are between the two nodes and what paths the data packets take. Network performance bottlenecks are marked in red on the topology map. You can locate a faulty network connection or a faulty network device by looking at red colored elements on the topology map.

When you click a node or hover over it on the topology map, you'll see the properties of the node like FQDN and IP address. Click a hop to see it's IP address. You can choose to filter particular routes by using the filters in the collapsible action pane. And, you can also simplify the network topologies by hiding the intermediate hops using the slider in the action pane. You can zoom-in or out of the topology map by using your mouse wheel.

Note that the topology shown in the map is layer 3 topology and doesn't contain layer 2 devices and connections.



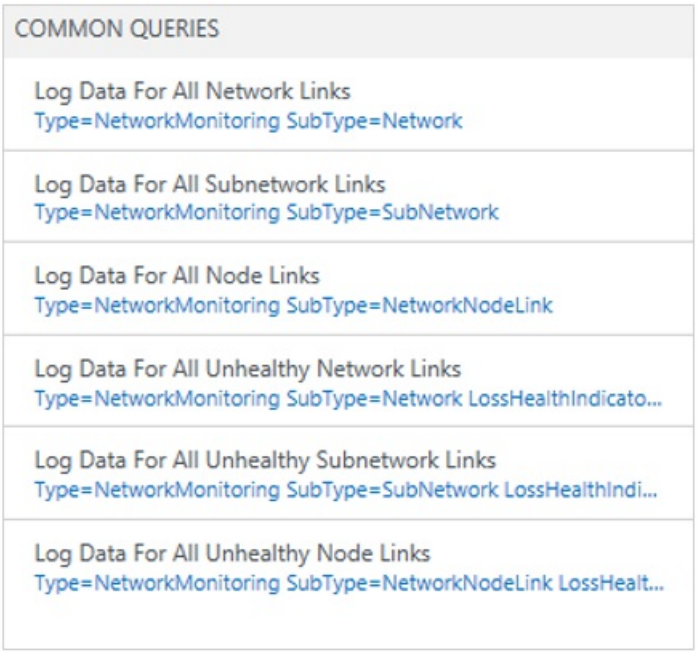
Fault localization

Network Performance Monitor is able to find the network bottlenecks without connecting to the network devices. Based on the data that it gathers from the network and by applying advanced algorithms on the network graph, Network Performance Monitor makes a probabilistic estimate of the parts of network that are most likely the source of the problem.

This approach is useful to determine the network bottlenecks when access to hops isn't available because it doesn't require any data to be gathered from the network devices such as routers or switches. This is also useful when the hops between two nodes are not in your administrative control. For example, the hops may be ISP routers.

Log Analytics search

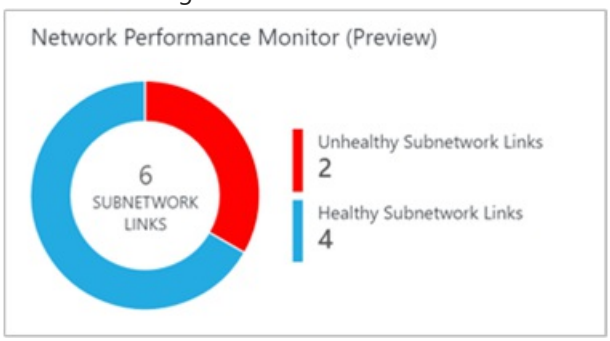
All data that is exposed graphically through the Network Performance Monitor dashboard and drill-down pages is also available natively in Log Analytics search. You can query the data using the search query language and create custom reports by exporting the data to Excel or PowerBI. The **Common Queries** blade in the dashboard has some useful queries that you can use as the starting point for creating your own queries and reports.



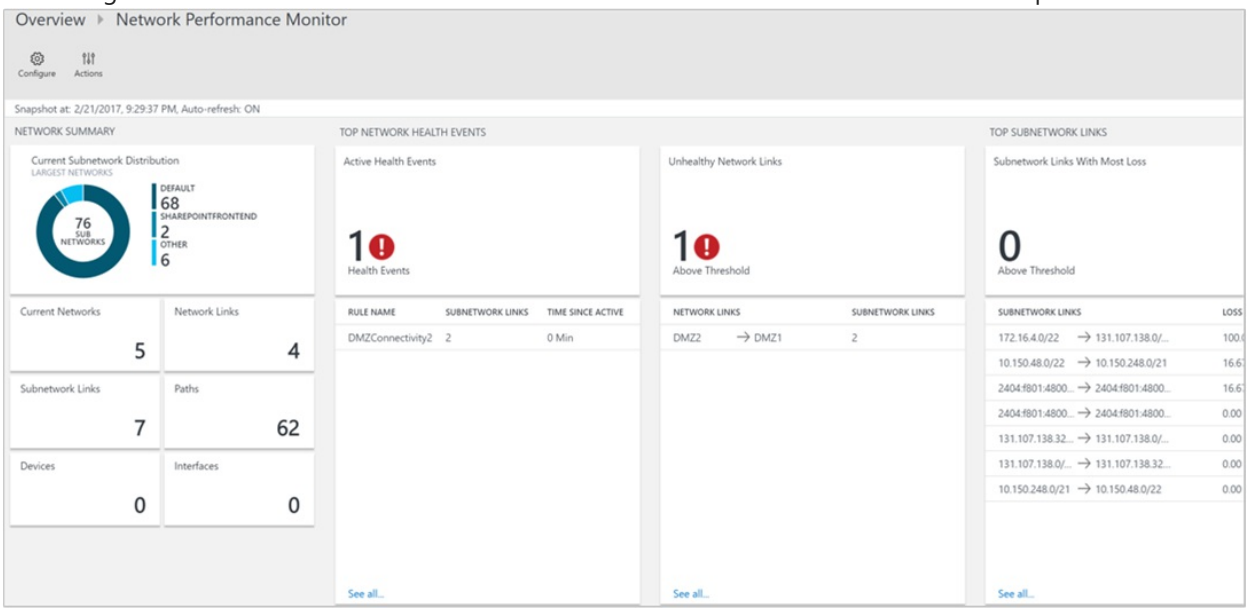
Investigate the root cause of a health alert

Now that you've read about Network Performance Monitor, let's look at a simple investigation into the root-cause for a health event.

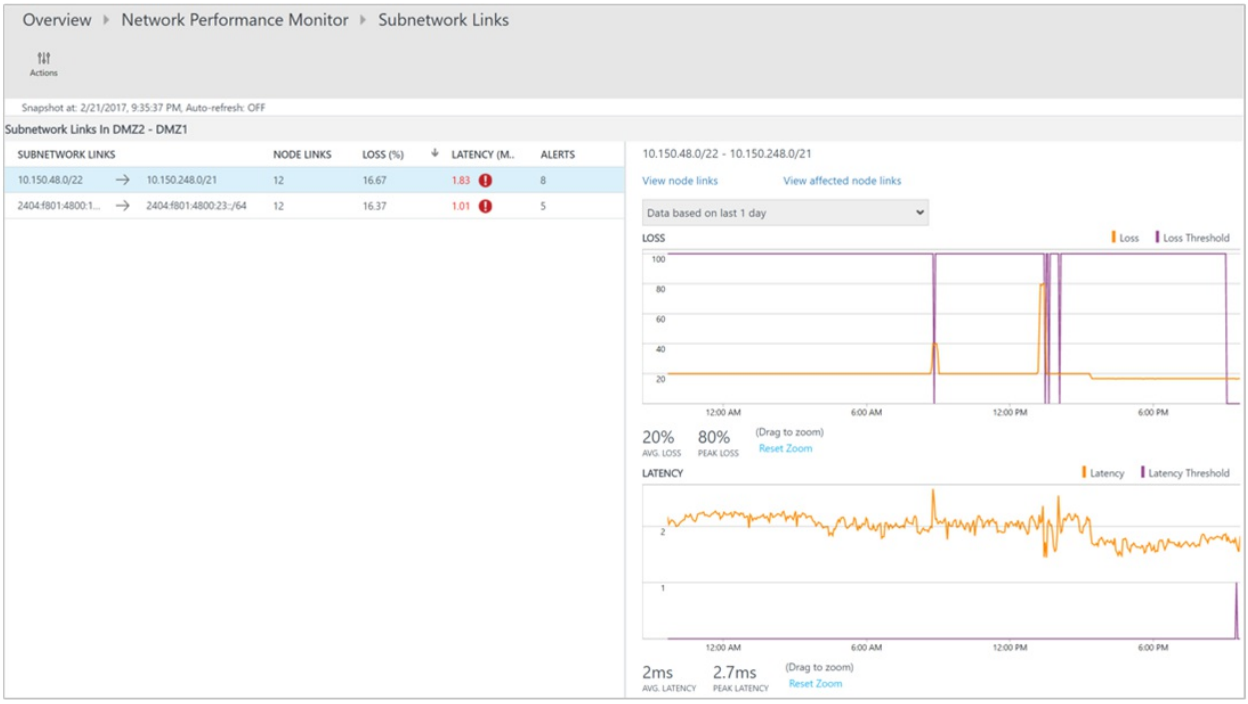
1. On the Overview page, you'll get a quick snapshot of the health of your network by observing the **Network Performance Monitor** tile. Notice that out of the 6 subnetworks links being monitored, 2 are unhealthy. This warrants investigation. Click the tile to view the solution dashboard.



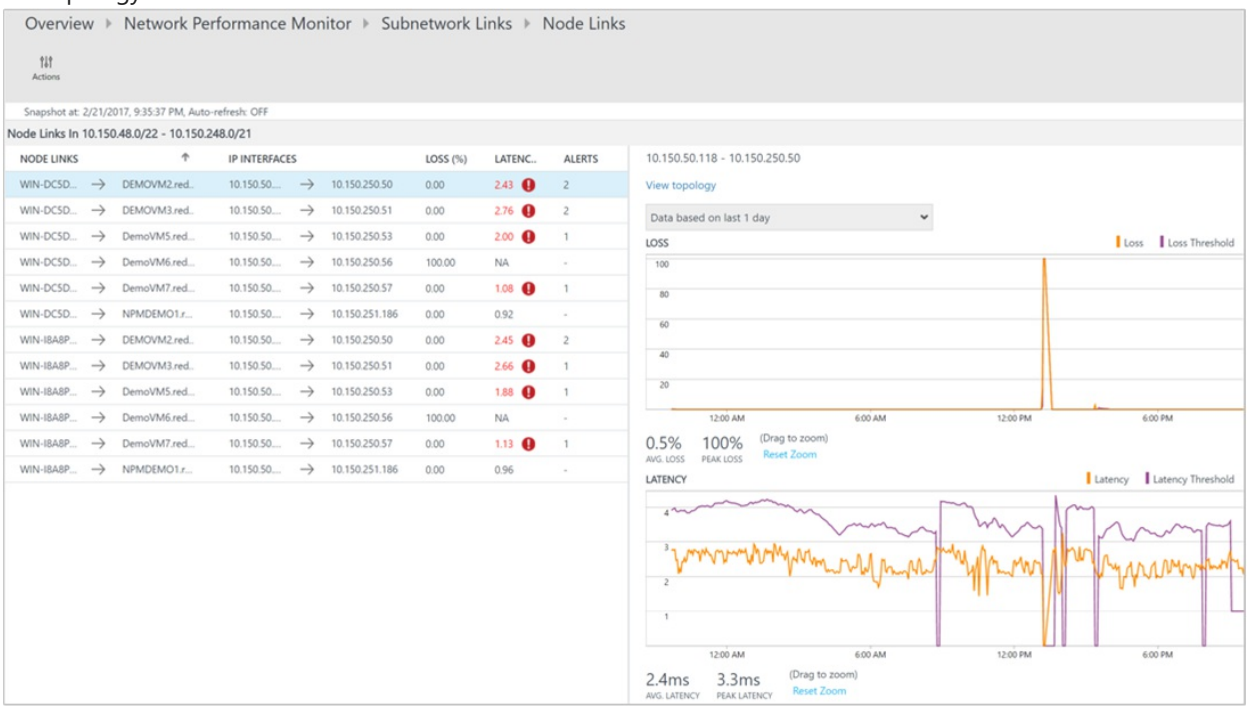
2. In the example image below, you'll notice that there is a health event a network link that is unhealthy. You decide to investigate the issue and click on the **DMZ2-DMZ1** network link to find out the root of the problem.



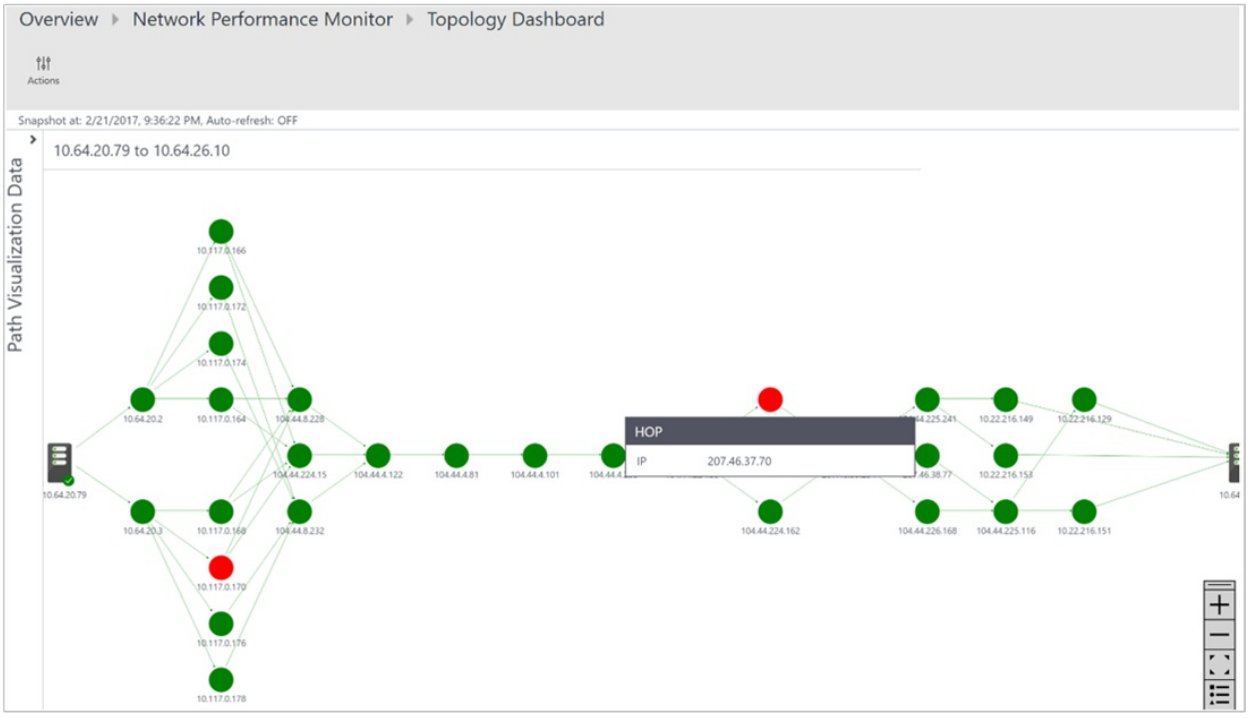
3. The drill-down page shows all the subnetwork links in **DMZ2-DMZ1** network link. You'll notice that for both the subnetwork links, the latency has crossed the threshold making the network link unhealthy. You can also see the latency trends of both the subnetwork links. You can use the time selection control in the graph to focus on the required time range. You can see the time of the day when latency has reached its peak. You can later search the logs for this time period to investigate the issue. Click **View node links** to drill-down further.



4. Similar to the previous page, the drill-down page for the particular subnetwork link lists down its constituent node links. You can perform similar actions here as you did in the previous step. Click **View topology** to view the topology between the 2 nodes.

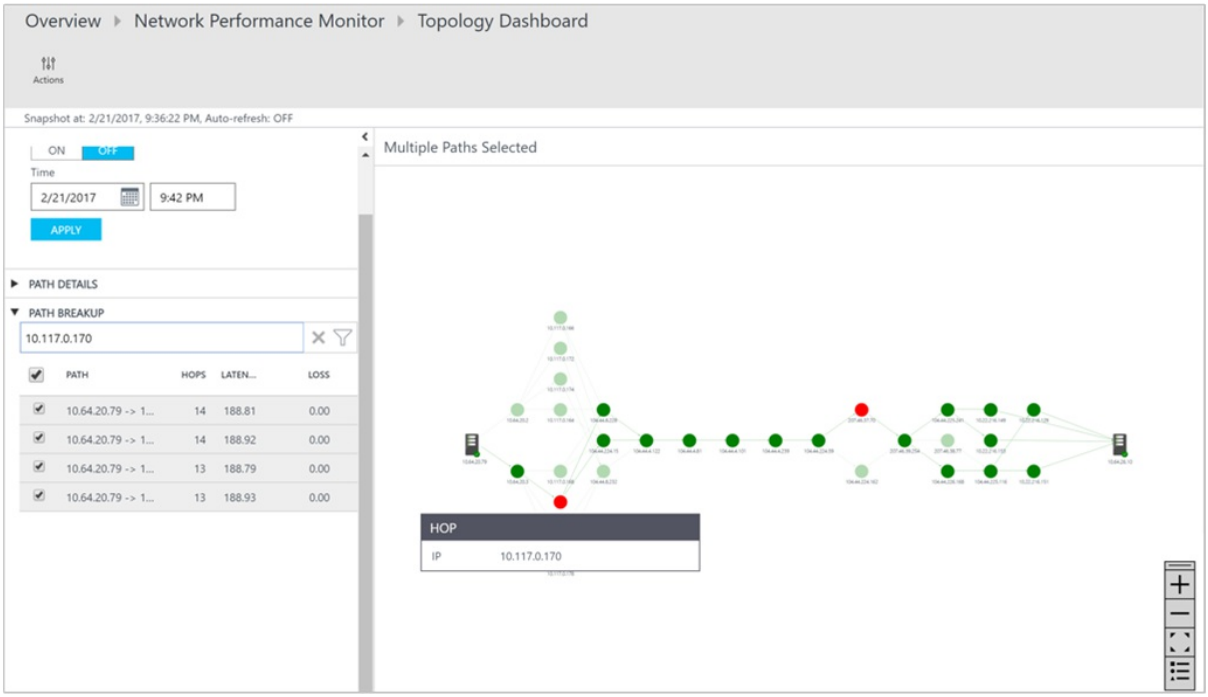


5. All the paths between the 2 selected nodes are plotted in the topology map. You can visualize the hop-by-hop topology of routes between two nodes on the topology map. It gives you a clear picture of how many routes exist between the two nodes and what paths the data packets are taking. Network performance bottlenecks are marked in red color. You can locate a faulty network connection or a faulty network device by looking at red colored elements on the topology map.



6. The loss, latency, and the number of hops in each path can be reviewed in the **Action** pane. Use the scrollbar to view the details of those unhealthy paths. Use the filters to select the paths with the unhealthy hop so that the topology for only the selected paths is plotted. You can use your mouse wheel to zoom in or out of the topology map.

   In the below image you can clearly see the root-cause of the problem areas to the specific section of the network by looking at the paths and hops in red color. Clicking on a node in the topology map reveals the properties of the node, including the FQDN, and IP address. Clicking on a hop shows the IP address of the hop.



Provide feedback

- **UserVoice** - You can post your ideas for Network Performance Monitor features that you want us to work on. Visit our UserVoice page.
- **Join our cohort** - We're always interested in having new customers join our cohort. As part of it, you'll get early access to new features and help us improve Network Performance Monitor. If you're interested in joining, fill-out this quick survey.

Next steps

- Search logs to view detailed network performance data records.

Assess Azure Service Fabric applications and micro-services with PowerShell

2/27/2017 • 13 min to read • Edit Online

This article describes how to use the Service Fabric solution in Log Analytics to help identify and troubleshoot issues across your Service Fabric cluster, by getting visibility into how your Service Fabric nodes are performing, and how your applications and micro-services are running.

The Service Fabric solution uses Azure Diagnostics data from your Service Fabric VMs, by collecting this data from your Azure WAD tables. Log Analytics then reads Service Fabric framework events, including **Reliable Service Events**, **Actor Events**, **Operational Events**, and **Custom ETW events**. The Service Fabric solution dashboard shows you notable issues and relevant events in your Service Fabric environment.

Installing and configuring the solution

Follow these three easy steps to install and configure the solution:

1. Ensure that the OMS workspace that you use is associated with the same Azure subscription that you used to create all cluster resources, including storage accounts. See Get started with Log Analytics for information about creating an OMS workspace.
2. Configure OMS to collect and view Service Fabric logs.
3. Enable the Service Fabric solution in your workspace.

Configure OMS to collect and view Service Fabric logs

In this section, you'll learn how to configure OMS to retrieve Service Fabric logs. The logs allow you view, analyze, and troubleshoot issues in your cluster or in the applications and services running in that cluster, using the OMS portal.

> **NOTE**
> The Azure Diagnostics extension must be configured to upload the logs to storage tables that match what OMS will look for. See How to collect logs with Azure Diagnostics for more information about how to collect logs. The configuration settings examples in this article show you what the names of the storage tables should be. Once Diagnostics is set up on the cluster and is uploading logs to a storage account, the next step is to configure OMS to collect these logs.

Ensure that you update the **EtwEventSourceProviderConfiguration** section in the **template.json** file to add entries for the new EventSources before you apply the configuration update by running **deploy.ps1**. The table for upload is the same as (ETWEventTable). At the moment, OMS can only read application ETW events from that table. However, support for custom ETW tables is in development.

The following tools are used to perform some of the operations in this section:

- Azure PowerShell
- Operations Management Suite

Configure an OMS workspace to show the cluster logs

After you've created an OMS workspace as described above, the next step is to configure the workspace to pull the logs from the Azure storage tables where they are being uploaded from the cluster by the Diagnostics extension. In order to do this, run the following PowerShell script:

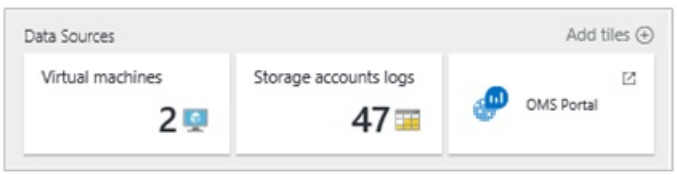
```
<#
    This script will configure an Operations Management Suite workspace (previously called an Operational
Insights workspace) to read Diagnostics from an Azure Storage account.
    It will enable all supported data types (currently Service Fabric Events, ETW Events and IIS Logs).
    It supports Resource Manager storage accounts.
    If you have more than one Azure Subscription, you will be prompted for the subscription to configure.
    If you have more than one OMS workspace you will be prompted for the workspace to configure.
    It will then look through your Service Fabric clusters, and configure your OMS workspace to read
Diagnostics from storage accounts that are connected to that cluster and have diagnostics enabled.
#>

try
{
    Get-AzureRMContext
}
catch [System.Management.Automation.PSInvalidOperationException]
{
    Add-AzureRmAccount
}

$validTables = "WADServiceFabric*EventTable", "WADETWEventTable"
function Select-Subscription {
      $subscription = ""
      $allSubscriptions = Get-AzureRmSubscription
      switch ($allSubscriptions.Count) {
             0 {Write-Error "No Operations Management Suite workspaces found"}
             1 {return $allSubscriptions}
        default {
            $uiPrompt = "Enter the number corresponding to the Azure subscription you would like to work
with.`n"

            $count = 1
            foreach ($subscription in $allSubscriptions) {
                $uiPrompt += "$count. " + $subscription.SubscriptionName + " (" + $subscription.SubscriptionId
+ ")`n"
                $count++
            }
            $answer = (Read-Host -Prompt $uiPrompt) - 1
            $subscription = $allSubscriptions[$answer]
             Write-Host $subscription.SubscriptionId
        }
    }
    return $subscription
}

function Select-Workspace {
    $workspace = ""
    $allWorkspaces = Get-AzureRmOperationalInsightsWorkspace

    switch ($allWorkspaces.Count) {
        0 {Write-Error "No Operations Management Suite workspaces found. `n"}
        1 {return $allWorkspaces}
        default {
            $uiPrompt = "Enter the number corresponding to the workspace you want to configure.`n"
            $count = 1
            foreach ($workspace in $allWorkspaces) {
                $uiPrompt += "$count. " + $workspace.Name + " (" + $workspace.CustomerId + ")`n"
                $count++
            }
            $answer = (Read-Host -Prompt $uiPrompt) - 1
            $workspace = $allWorkspaces[$answer]
             Write-Host $workspace.WorkspaceName
        }
    }
    return $workspace
}

function Check-ETWProviderLogging {
```

```
     param(
     [string]$id,
     [string]$provider,
     [string]$expectedTable,
     [string]$table
    )
         Write-Debug ("ID: $id Provider: $provider ExpectedTable $expectedTable ActualTable $table")
         if ( ($table -eq $null) -or ($table -eq ""))
         {
             Write-Warning ("$id No configuration found for $provider. Configure Azure diagnostics to write to
$expectedTable.")
         }
         elseif ( $table -ne $expectedTable )
         {
             Write-Warning ("$id $provider events are being written to $table instead of WAD$expectedTable.
Events will not be collected by OMS")
         }
         else
         {
             Write-Verbose "$id $provider events are being written to WAD$expectedTable (Correct
configuration.)"
         }
 }

function Check-ServiceFabricScaleSetDiagnostics {
     param(
          [psobject]$scaleSetDiagnostics
   )
     $storageAccountsFound = @()
     Write-Verbose ("Checking " + $scaleSetDiagnostics)
     $sfReliableActorTable = $null
     $sfReliableServiceTable = $null
     $sfOperationalTable = $null

     Write-Debug $scaleSetDiagnostics
     $serviceFabricProviderList = ""
     $etwManifestProviderList = ""

     if ( $scaleSetDiagnostics.xmlCfg )
      {
             Write-Debug ("Found XMLcfg")
             $xmlCfg =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($scaleSetDiagnostics.xmlCfg))
             Write-Debug $xmlCfg
             $etwProviders = Select-Xml -Content $xmlCfg -XPath "//EtwProviders"
             $serviceFabricProviderList = $etwProviders.Node.EtwEventSourceProviderConfiguration
             $etwManifestProviderList = $etwProviders.Node.EtwManifestProviderConfiguration
      } elseif ($scaleSetDiagnostics.WadCfg )
     {
         Write-Debug ("Found WADcfg")
         Write-Debug $scaleSetDiagnostics.WadCfg
         $serviceFabricProviderList =
$scaleSetDiagnostics.WadCfg.DiagnosticMonitorConfiguration.EtwProviders.EtwEventSourceProviderConfiguration
         $etwManifestProviderList =
$scaleSetDiagnostics.WadCfg.DiagnosticMonitorConfiguration.EtwProviders.EtwManifestProviderConfiguration
     } else
     {
         Write-Error "Unable to parse Azure Diagnostics setting for $id"
             Write-Warning ("$id does not have diagnostics enabled")
     }
     foreach ($provider in $serviceFabricProviderList)
     {
         Write-Debug ("Event Source Provider: " + $provider.Provider + " Destination: " +
$provider.DefaultEvents.eventDestination)
         if ($provider.Provider -eq "Microsoft-ServiceFabric-Actors")
         {
             $sfReliableActorTable = $provider.DefaultEvents.eventDestination
         } elseif ($provider.Provider -eq "Microsoft-ServiceFabric-Services")
         {
```

```
            {
                $sfReliableServiceTable = $provider.DefaultEvents.eventDestination
            } else
            {
                Check-ETWProviderLogging $id $provider.Provider "ETWEventTable"
$provider.DefaultEvents.eventDestination
            }
        }
        foreach ($provider in $etwManifestProviderList)
        {
            Write-Debug ("Manifest Provider: " + $provider.Provider + " Destination: " +
$provider.DefaultEvents.eventDestination)
            if ($provider.Provider -eq "cbd93bc2-71e5-4566-b3a7-595d8eeca6e8")
            {
                $sfOperationalTable = $provider.DefaultEvents.eventDestination
            } else
            {
                Check-ETWProviderLogging $id $provider.Provider "ETWEventTable"
$provider.DefaultEvents.eventDestination
            }
        }

        Check-ETWProviderLogging $id "Microsoft-ServiceFabric-Actors" "ServiceFabricReliableActorEventTable"
$sfReliableActorTable
        Check-ETWProviderLogging $id "Microsoft-ServiceFabric-Services" "ServiceFabricReliableServiceEventTable"
$sfReliableServiceTable
        Check-ETWProviderLogging $id "cbd93bc2-71e5-4566-b3a7-595d8eeca6e8 (System events)"
"ServiceFabricSystemEventTable" $sfOperationalTable

        Write-Verbose ("StorageAccount: " + $scaleSetDiagnostics.StorageAccount)
        $storageAccountsFound += ($scaleSetDiagnostics.StorageAccount)
        return ($storageAccountsFound)
    }

function Select-StorageAccount {
    $allResources = Get-AzureRmResource #pulls in all resources
    $serviceFabricClusters = $allResources.Where({$_.ResourceType -eq "Microsoft.ServiceFabric/clusters"})
#pulls in all service fabric clusters in the resource
    $storageAccountList = @()
    foreach($cluster in $serviceFabricClusters) {
        Write-Host("Checking cluster: " + $cluster.Name)
         $scaleSet = $allResources.Where({($_.ResourceType -eq "Microsoft.Compute/virtualMachineScaleSets") -
and ($_.ResourceGroupName -eq $cluster.ResourceGroupName)})

         foreach($set in $scaleSet) {
             $resource = Get-AzureRmResource -ResourceId $set.ResourceId
             $extensions = $resource.Properties.VirtualMachineProfile.ExtensionProfile.Extensions

             foreach($ext in $extensions) {
                 if ($ext.Properties.Publisher -eq "Microsoft.Azure.Diagnostics" -and $ext.Properties.Type -eq
"IaaSDiagnostics") {
                     $storageAccountList += (Check-ServiceFabricScaleSetDiagnostics $ext.Properties.Settings)
                 }
             }
          }

         $storageAccountsToCheck = $allResources.Where({($_.ResourceType -eq
"Microsoft.Storage/storageAccounts") -and ($_.ResourceName -in $storageAccountList)})

         if ($storageAccountsToCheck.Count -eq "0") {
                Write-Error "No storage accounts found"
           }
           else {
                    foreach ($storageAccount in $storageAccountsToCheck) {
                        Write-Host("Checking Storage Account: " + $storageAccount.Name)
                        $insightsName = $storageAccount.Name + $workspace.Name
                        $existingConfig = ""
                        try
                            {
                                $existingConfig = Get-AzureRmOperationalInsightsStorageInsight -Workspace
```

```
                                $existingConfig = Get-AzureRmOperationalInsightsStorageInsight -Workspace
$workspace -Name $insightsName -ErrorAction Stop
                            }
                        catch [Hyak.Common.CloudException]
                            {
                                # HTTP Not Found is returned if the storage insight doesn't exist
                            }
                        if ($existingConfig) {
                                  [array]$Tables = $existingConfig.Tables
                                   foreach($table in $validTables) {
                                         if($Tables -notcontains $table) {
                                               $Tables += $table
                                               $dirty = $true;
                                               Write-Host "Adding Table: $table";
                                         }
                                         else {
                                               Write-Host "$table is already configured.`n";
                                            }
                                      }
                                      # If any of the tables from the table list are not already monitored,
then we add them
                                    if($dirty -eq $true) {
                                           Set-AzureRmOperationalInsightsStorageInsight -Workspace $workspace -
Name $insightsName -Tables $Tables
                                           Write-Host "Updating Storage Insight. `n"
                                     }
                                     else {
                                           Write-Host "Storage Insight already updated."
                                    }
                               }
                     else {
                            $key = (Get-AzureRmStorageAccountKey -ResourceGroupName
$storageAccount.ResourceGroupName -Name $storageAccount.Name)[0].Value
                           New-AzureRmOperationalInsightsStorageInsight -Workspace $workspace -Name
$insightsName -StorageAccountResourceId $storageAccount.ResourceId -StorageAccountKey $key -Tables $validTables
                            Write-Host "New Azure Storage Insight Configured. `n"
                           }
                  }
             }
      }
      return
     }

$subscription = Select-Subscription
$subscriptionId = $subscription.SubscriptionId
$subscription = Select-AzureRmSubscription -SubscriptionId $subscriptionId
$workspace = Select-Workspace
$storageAccount = Select-StorageAccount
```

After you've configured the OMS workspace to read from the Azure tables in your storage account, log into the Azure portal, and select the OMS Workspace from **All Resources**. Once selected, you should see the number of storage account logs connected to that OMS Workspace. Select the **Storage account logs** tile and verify from the list of storage account logs that your storage account is connected to that OMS workspace:

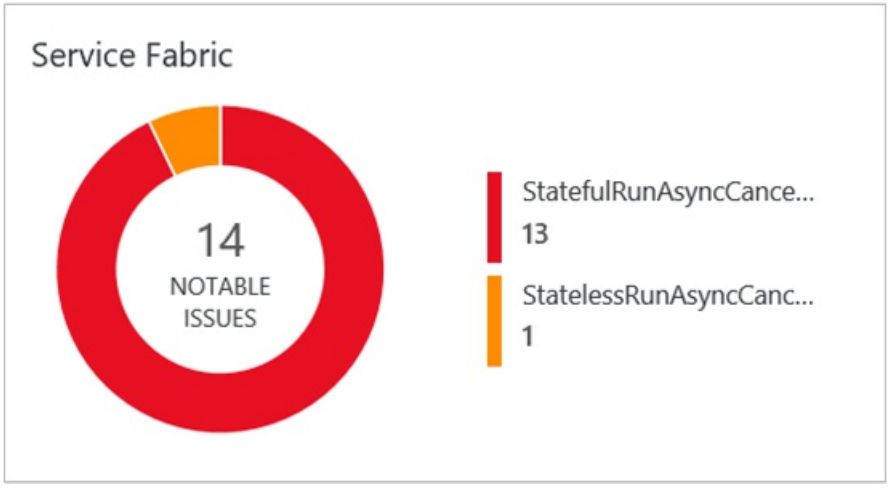


Enable the Service Fabric solution

Use the following script to add the solution to your OMS workspace. Run the script in PowerShell, using the Azure subscription that is associated with the OMS workspace that you want to enable the Service Fabric solution in.

```
function Select-Subscription {
      $subscription = ""
      $allSubscriptions = Get-AzureRmSubscription
      switch ($allSubscriptions.Count) {
             0 {Write-Error "No Operations Management Suite workspaces found"}
             1 {return $allSubscriptions}
        default {
            $uiPrompt = "Enter the number corresponding to the Azure subscription you would like to work
with.`n"
            $count = 1
            foreach ($subscription in $allSubscriptions) {
                $uiPrompt += "$count. " + $subscription.SubscriptionName + " (" + $subscription.SubscriptionId
+ ")`n"
                $count++
            }
            $answer = (Read-Host -Prompt $uiPrompt) - 1
            $subscription = $allSubscriptions[$answer]
             Write-Host $subscription.SubscriptionId
        }
    }
    return $subscription
}

function Select-Workspace {
    $workspace = ""
    $allWorkspaces = Get-AzureRmOperationalInsightsWorkspace
    switch ($allWorkspaces.Count) {
        0 {Write-Error "No Operations Management Suite workspaces found"}
        1 {return $allWorkspaces}
        default {
            $uiPrompt = "Enter the number corresponding to the workspace you want to configure.`n"
            $count = 1
            foreach ($workspace in $allWorkspaces) {
                $uiPrompt += "$count. " + $workspace.Name + " (" + $workspace.CustomerId + ")`n"
                $count++
            }
            $answer = (Read-Host -Prompt $uiPrompt) - 1
            $workspace = $allWorkspaces[$answer]
                          Write-Host $workspace.WorkspaceName
        }
    }
    return $workspace
}
$subscription = Select-Subscription
$subscriptionId = $subscription.SubscriptionId
$subscription = Select-AzureRmSubscription -SubscriptionId $subscriptionId
$workspace = Select-Workspace
Set-AzureRmOperationalInsightsIntelligencePack -ResourceGroupName $workspace.ResourceGroupName -WorkspaceName
$workspace.Name -IntelligencePackName "ServiceFabric" -Enabled $true
```

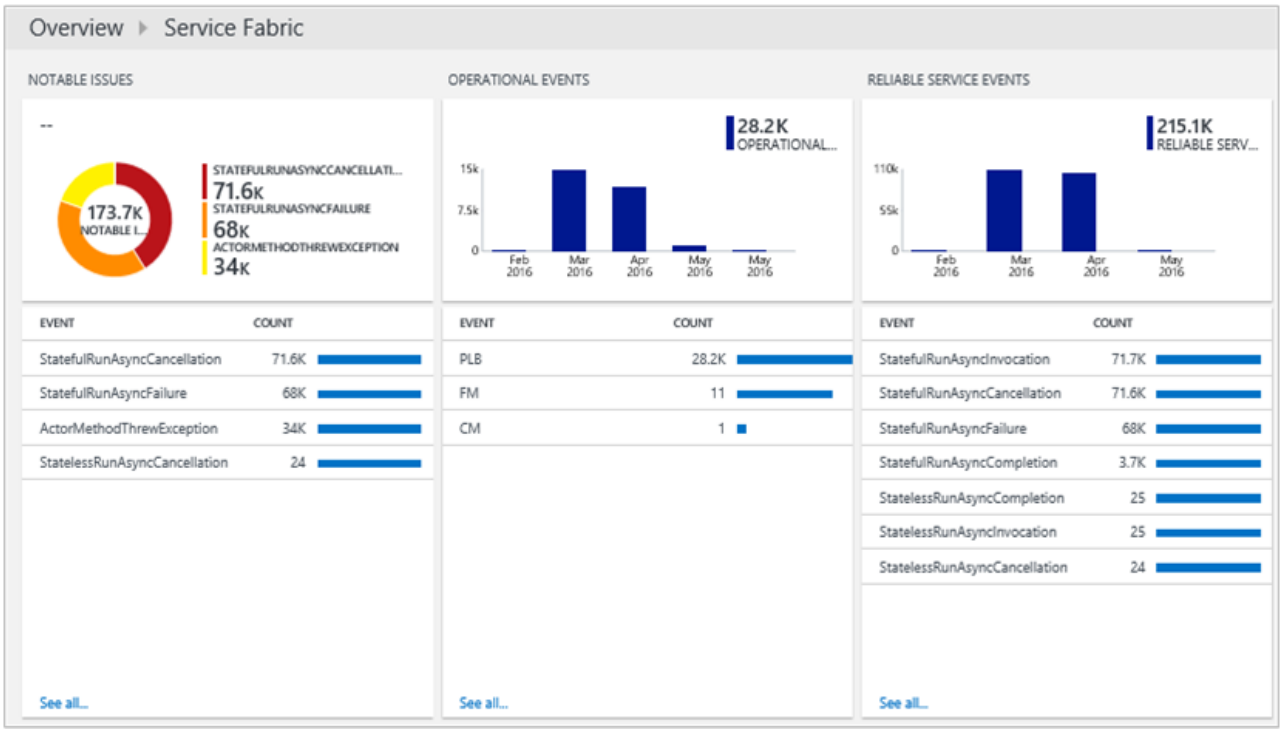
After the solution is enabled, the Service Fabric tile is added to your OMS Overview page, with a view of notable issues such as runAsync failures and cancellations that have occurred in the last 24 hours.

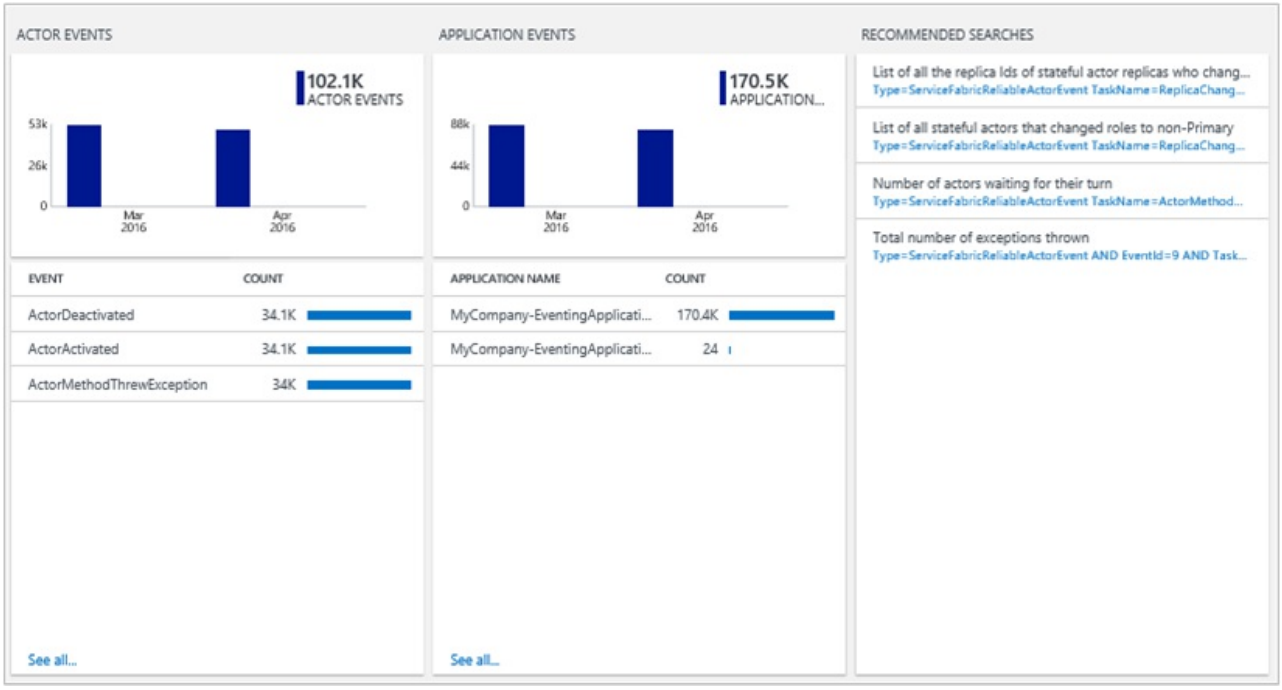


View Service Fabric events

Click the **Service Fabric** tile to open the Service Fabric dashboard. The dashboard includes the columns in the following table. Each column lists the top ten events by count matching that column's criteria for the specified time range. You can run a log search that provides the entire list by clicking **See all** at the right bottom of each column, or by clicking the column header.

SERVICE FABRIC EVENT	DESCRIPTION
Notable Issues	A Display of issues such as RunAsyncFailures RunAsynCancellations and Node Downs.
Operational Events	Notable operational events such as application upgrade and deployments.
Reliable Service Events	Notable reliable service events such a Runasyncinvocations.
Actor Events	Notable actor events generated by your micro-services, such as exceptions thrown by an actor method, actor activations and deactivations, and so on.
Application Events	All custom ETW events generated by your applications.





The following table shows data collection methods and other details about how data is collected for Service Fabric.

PLATFORM	DIRECT AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows	✗	✗	●	✗	✗	10 minutes

> **NOTE**
>
> You can change the scope of these events in the Service Fabric solution by clicking **Data based on last 7 days** at the top of the dashboard. You can also show events generated within the last 7 days, 1 day, or 6 hours. Or, you can select **Custom** to specify a custom date range.

Troubleshoot your Service Fabric and OMS configuration

If you need to verify your OMS configuration because you are unable to view event data in OMS, use the script below. It reads your Service Fabric diagnostics configuration, checks for data being written into the tables, and it verifies that OMS is configured to read from the tables.

```
<#
    Verify Service Fabric and OMS configuration
    1. Read Service Fabric diagnostics configuration
    2. Check for data being written into the tables
    3. Verify OMS is configured to read from the tables

    Supported tables:
    WADServiceFabricReliableActorEventTable
    WADServiceFabricReliableServiceEventTable
    WADServiceFabricSystemEventTable
    WADETWEventTable

    Script will write a warning for every misconfiguration detected
    To see items that are correctly configured set $VerbosePreference="Continue"
#>
Param
(
```

```
    [Parameter(Mandatory=$true,
    ValueFromPipeline=$true,
    Position=1)]
    [string]$workspaceName
)

$WADtables = @("WADServiceFabricReliableActorEventTable",
               "WADServiceFabricReliableServiceEventTable",
               "WADServiceFabricSystemEventTable",
               "WADETWEventTable"
               )

<#
    Check if OMS Log Analytics is configured to index service fabric events from the specified table
#>

function Check-OMSLogAnalyticsConfiguration {
    param(
    [psobject]$workspace,
    [psobject]$storageAccount,
    [string]$id
    )

    $existingInsights = Get-AzureRmOperationalInsightsStorageInsight -ResourceGroupName
$workspace.ResourceGroupName -WorkspaceName $workspace.Name

    if ($existingInsights)
    {
        $currentStorageAccountInsight = $existingInsights.Where({$_.StorageAccountResourceId -eq
$storageAccount.ResourceId})

        if ("WADServiceFabric*EventTable" -in $currentStorageAccountInsight.Tables)
        {
            Write-Verbose ("OMS Log Analytics workspace " + $workspace.Name + " is configured to index service
fabric actor, service and operational events from " + $storageAccount.Name)
        } else
        {
            Write-Warning ("OMS Log Analytics workspace " + $workspace.Name + " is not configured to index
service fabric actor, service and operational events from " + $storageAccount.Name)
        }
        if ("WADETWEventTable" -in $currentStorageAccountInsight.Tables)
        {
            Write-Verbose ("OMS Log Analytics workspace " + $workspace.Name + " is configured to index service
fabric application events from " + $storageAccount.Name)
        } else
        {
            Write-Warning ("OMS Log Analytics workspace " + $workspace.Name + " is not configured to index
service fabric application events from " + $storageAccount.Name)
        }
    } else
    {
        Write-Warning ("OMS Log Analytics workspace " + $workspace.Name + "is not configured to read service
fabric events from " + $storageAccount.Name)
    }
}

<#
    Check Azure table storage to confirm there is recent data written by Service Fabric
#>

function Check-TablesForData {
    param(
    [psobject]$storageAccount
    )

    $ctx = (Get-AzureRmStorageAccount -ResourceGroupName $storageAccount.ResourceGroupName -Name
$storageAccount.ResourceName).Context

    $createdTables = Get-AzureStorageTable -Context $ctx
```

```
    $recently = Get-Date -Format s ((Get-Date).AddMinutes(-20).ToUniversalTime())
    $recently = $recently + "Z"

    foreach ($table in $WADtables)
    {
        if ($table -in $createdTables.Name)
        {
            $tbl = Get-AzureStorageTable -Name $table -Context $ctx
            $query = New-Object Microsoft.WindowsAzure.Storage.Table.TableQuery
            $list = New-Object System.Collections.Generic.List[string]
            $list.Add("RowKey")
            $list.Add("ProviderName")
            $list.Add("Timestamp")
            $query.FilterString = "Timestamp gt datetime'$recently'"
            $query.SelectColumns = $list
            $query.TakeCount = 20
            $entities = $tbl.CloudTable.ExecuteQuery($query)
            Write-Debug $entities
            if ($entities.Count -gt 0)
            {
                Write-Verbose ("Data was written to $table in " + $storageAccount.ResourceName + "after
$recently")
            } else
            {
                Write-Warning ("No data after $recently is in  $table in " + $storageAccount.ResourceName)
            }
        } else
        {
            Write-Warning ("$table does not exist in storage account " + $storageAccount.ResourceName)
        }
    }
}

<#
    Check if ETW provider is configured to log events to the expected table storage
#>
function Check-ETWProviderLogging {
    param(
    [string]$id,
    [string]$provider,
    [string]$expectedTable,
    [string]$table
    )
        Write-Debug ("ID: $id Provider: $provider ExpectedTable $expectedTable ActualTable $table")
        if ( ($table -eq $null) -or ($table -eq ""))
        {
            Write-Warning ("$id No configuration found for $provider. Configure Azure diagnostics to write to
$expectedTable.")
        }
        elseif ( $table -ne $expectedTable )
        {
            Write-Warning ("$id $provider events are being written to $table instead of WAD$expectedTable.
Events will not be collected by OMS")
        }
        else
        {
            Write-Verbose "$id $provider events are being written to WAD$expectedTable (Correct
configuration.)"
        }
}

<#
    Check Azure Diagnostics Configuration for a Service Fabric cluster
#>
function Check-ServiceFabricScaleSetDiagnostics {
    param(
    [psobject]$scaleSetDiagnostics
    )
```

```
    $storageAccountsFound = @()
    Write-Verbose ("Checking " + $scaleSetDiagnostics)
    $sfReliableActorTable = $null
    $sfReliableServiceTable = $null
    $sfOperationalTable = $null
    Write-Debug $scaleSetDiagnostics
    $serviceFabricProviderList = ""
    $etwManifestProviderList = ""

    if ( $scaleSetDiagnostics.xmlCfg )
    {
        Write-Debug ("Found XMLcfg")
        $xmlCfg =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($scaleSetDiagnostics.xmlCfg))
        Write-Debug $xmlCfg
        $etwProviders = Select-Xml -Content $xmlCfg -XPath "//EtwProviders"
        $serviceFabricProviderList = $etwProviders.Node.EtwEventSourceProviderConfiguration
        $etwManifestProviderList = $etwProviders.Node.EtwManifestProviderConfiguration
    } elseif ($scaleSetDiagnostics.WadCfg )
    {
        Write-Debug ("Found WADcfg")
        Write-Debug $scaleSetDiagnostics.WadCfg
        $serviceFabricProviderList =
$scaleSetDiagnostics.WadCfg.DiagnosticMonitorConfiguration.EtwProviders.EtwEventSourceProviderConfiguration
        $etwManifestProviderList =
$scaleSetDiagnostics.WadCfg.DiagnosticMonitorConfiguration.EtwProviders.EtwManifestProviderConfiguration
    } else
    {
        Write-Error "Unable to parse Azure Diagnostics setting for $id"
        Write-Warning ("$id does not have diagnostics enabled")
    }

    foreach ($provider in $serviceFabricProviderList)
    {
        Write-Debug ("Event Source Provider: " + $provider.Provider + " Destination: " +
$provider.DefaultEvents.eventDestination)
        if ($provider.Provider -eq "Microsoft-ServiceFabric-Actors")
        {
            $sfReliableActorTable = $provider.DefaultEvents.eventDestination
        } elseif ($provider.Provider -eq "Microsoft-ServiceFabric-Services")
        {
            $sfReliableServiceTable = $provider.DefaultEvents.eventDestination
        } else
        {
            Check-ETWProviderLogging $id $provider.Provider "ETWEventTable"
$provider.DefaultEvents.eventDestination
        }
    }
    foreach ($provider in $etwManifestProviderList)
    {
        Write-Debug ("Manifest Provider: " + $provider.Provider + " Destination: " +
$provider.DefaultEvents.eventDestination)
        if ($provider.Provider -eq "cbd93bc2-71e5-4566-b3a7-595d8eeca6e8")
        {
            $sfOperationalTable = $provider.DefaultEvents.eventDestination
        } else
        {
            Check-ETWProviderLogging $id $provider.Provider "ETWEventTable"
$provider.DefaultEvents.eventDestination
        }
    }

    Check-ETWProviderLogging $id "Microsoft-ServiceFabric-Actors" "ServiceFabricReliableActorEventTable"
$sfReliableActorTable
    Check-ETWProviderLogging $id "Microsoft-ServiceFabric-Services" "ServiceFabricReliableServiceEventTable"
$sfReliableServiceTable
    Check-ETWProviderLogging $id "cbd93bc2-71e5-4566-b3a7-595d8eeca6e8 (System events)"
"ServiceFabricSystemEventTable" $sfOperationalTable
```

```
    Write-Verbose ("StorageAccount: " + $scaleSetDiagnostics.StorageAccount)

    $storageAccountsFound += ($scaleSetDiagnostics.StorageAccount)
    return ($storageAccountsFound)
}

# This script uses Get-AzureRmVMDiagnosticsExtension and needs a version where -Name is not a required
parameter
Import-Module AzureRM.Compute -MinimumVersion 1.2.2

try
{
    Get-AzureRmContext
}
catch [System.Management.Automation.PSInvalidOperationException]
{
    Login-AzureRmAccount
}

$allResources = Get-AzureRmResource

$OMSworkspace = $allResources.Where({($_.ResourceType -eq "Microsoft.OperationalInsights/workspaces") -and
($_.ResourceName -eq $workspaceName)})

if ($OMSworkspace.Name -ne $workspaceName)
{
    Write-Error ("Unable to find OMS Workspace " + $workspaceName)
}

$serviceFabricClusters = $allResources.Where({$_.ResourceType -eq "Microsoft.ServiceFabric/clusters"})
$storageAccountList = @()
foreach($cluster in $serviceFabricClusters) {
    Write-Verbose ("Checking cluster: " + $cluster.Name)
    $scaleSet = ($allResources.Where({($_.ResourceType -eq "Microsoft.Compute/virtualMachineScaleSets") -and
($_.ResourceGroupName -eq $cluster.ResourceGroupName)}))

    foreach($set in $scaleSet) {
        $resource = Get-AzureRmResource -ResourceId $set.ResourceId
        $extensions = $resource.Properties.VirtualMachineProfile.ExtensionProfile.Extensions
        foreach($ext in $extensions) {
            if ($ext.Properties.Publisher -eq "Microsoft.Azure.Diagnostics" -and $ext.Properties.Type -eq
"IaaSDiagnostics") {
                $storageAccountList += (Check-ServiceFabricScaleSetDiagnostics $ext.Properties.Settings)
            }
        }
    }
}

$storageAccountList = $storageAccountList | Sort-Object | Get-Unique
$storageAccountsToCheck = ($allResources.Where({($_.ResourceType -eq "Microsoft.Storage/storageAccounts") -and
($_.ResourceName -in $storageAccountList)}))

foreach($storageAccount in $storageAccountsToCheck)
{
    Check-TablesForData $storageAccount
    Check-OMSLogAnalyticsConfiguration $OMSworkspace $storageAccount
}
```

Next steps

- Use Log Searches in Log Analytics to view detailed Service Fabric event data.

Optimize your SQL Server environment with the SQL Assessment solution in Log Analytics

4/13/2017 • 10 min to read • Edit Online

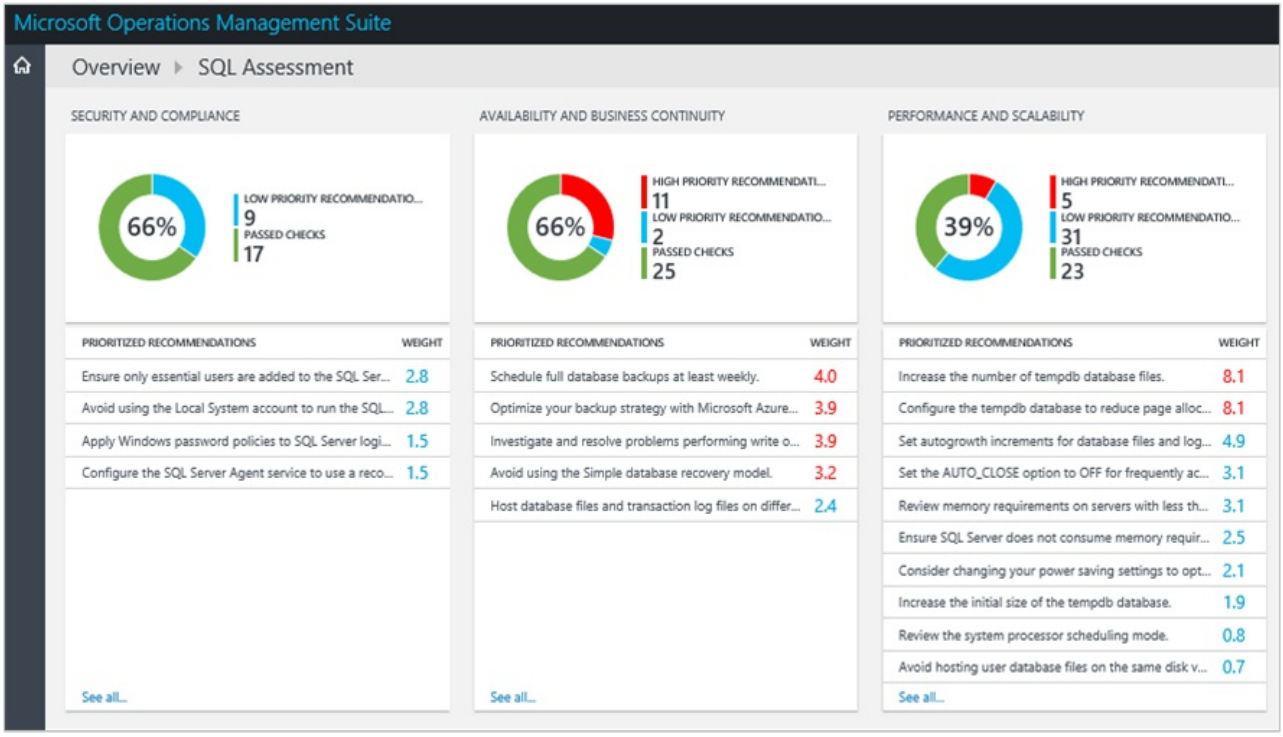
You can use the SQL Assessment solution to assess the risk and health of your server environments on a regular interval. This article will help you install the solution so that you can take corrective actions for potential problems.

This solution provides a prioritized list of recommendations specific to your deployed server infrastructure. The recommendations are categorized across six focus areas which help you quickly understand the risk and take corrective action.

The recommendations made are based on the knowledge and experience gained by Microsoft engineers from thousands of customer visits. Each recommendation provides guidance about why an issue might matter to you and how to implement the suggested changes.

You can choose focus areas that are most important to your organization and track your progress toward running a risk free and healthy environment.

After you've added the solution and an assessment is completed, summary information for focus areas is shown on the **SQL Assessment** dashboard for the infrastructure in your environment. The following sections describe how to use the information on the **SQL Assessment** dashboard, where you can view and then take recommended actions for your SQL server infrastructure.



Installing and configuring the solution

SQL Assessment works with all currently supported versions of SQL Server for the Standard, Developer, and Enterprise editions.

Use the following information to install and configure the solution.

- Agents must be installed on servers that have SQL Server installed.
- The SQL Assessment solution requires a supported version of .NET Framework 4 installed on each computer that has an OMS agent.
- In order to install the solution, the user must be an administrator or contributor to the Azure subscription when using the Azure portal. In addition, the user must be a member of the OMS workspace contributor or administrator role in the OMS portal.
- When using the Operations Manager agent with SQL Assessment, you'll need to use an Operations Manager Run-As account. See Operations Manager run-as accounts for OMS below for more information.

  > **NOTE**
  > The MMA agent does not support Operations Manager Run-As accounts.

- Add the SQL Assessment solution to your OMS workspace using the process described in Add Log Analytics solutions from the Solutions Gallery. There is no further configuration required.

> **NOTE**
> After you've added the solution, the AdvisorAssessment.exe file is added to servers with agents. Configuration data is read and then sent to the OMS service in the cloud for processing. Logic is applied to the received data and the cloud service records the data.

SQL Assessment data collection details

SQL Assessment collects WMI data, registry data, performance data, and SQL Server dynamic management view results using the agents that you have enabled.

The following table shows data collection methods for agents, whether Operations Manager (SCOM) is required, and how often data is collected by an agent.

PLATFORM	DIRECT AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows	✓	✓	✗	✗	✓	7 days

Operations Manager run-as accounts for OMS

Log Analytics in OMS uses the Operations Manager agent and management group to collect and send data to the OMS service. OMS builds upon management packs for workloads to provide value-add services. Each workload requires workload-specific privileges to run management packs in a different security context, such as a domain account. You need to provide credential information by configuring an Operations Manager Run As account.

Use the following information to set the Operations Manager run-as account for SQL Assessment.

Set the Run As account for SQL assessment

If you are already using the SQL Server management pack, you should use that Run As account.

To configure the SQL Run As account in the Operations console

> **NOTE**
> If you are using the OMS direct agent, rather than the SCOM agent, the management pack always runs in the security context of the Local System account. Skip steps 1-5 below, and run either the T-SQL or Powershell sample, specifying NT AUTHORITY\SYSTEM as the user name.

1. In Operations Manager, open the Operations console, and then click **Administration**.
2. Under **Run As Configuration**, click **Profiles**, and open **OMS SQL Assessment Run As Profile**.
3. On the **Run As Accounts** page, click **Add**.
4. Select a Windows Run As account that contains the credentials needed for SQL Server, or click **New** to create one.

   > **NOTE**
   > The Run As account type must be Windows. The Run As account must also be part of Local Administrators group on all Windows Servers hosting SQL Server Instances.

5. Click **Save**.
6. Modify and then execute the following T-SQL sample on each SQL Server Instance to grant minimum permissions required to Run As Account to perform SQL Assessment. However, you don't need to do this if a Run As Account is already part of the sysadmin server role on SQL Server Instances.

```
---
    -- Replace <UserName> with the actual user name being used as Run As Account.
    USE master

    -- Create login for the user, comment this line if login is already created.
    CREATE LOGIN [<UserName>] FROM WINDOWS

    -- Grant permissions to user.
    GRANT VIEW SERVER STATE TO [<UserName>]
    GRANT VIEW ANY DEFINITION TO [<UserName>]
    GRANT VIEW ANY DATABASE TO [<UserName>]

    -- Add database user for all the databases on SQL Server Instance, this is required for connecting to
individual databases.
    -- NOTE: This command must be run anytime new databases are added to SQL Server instances.
    EXEC sp_msforeachdb N'USE [?]; CREATE USER [<UserName>] FOR LOGIN [<UserName>];'
```

To configure the SQL Run As account using Windows PowerShell

Open a PowerShell window and run the following script after you've updated it with your information:

```
    import-module OperationsManager
    New-SCOMManagementGroupConnection "<your management group name>"

    $profile = Get-SCOMRunAsProfile -DisplayName "OMS SQL Assessment Run As Profile"
    $account = Get-SCOMrunAsAccount | Where-Object {$_.Name -eq "<your run as account name>"}
    Set-SCOMRunAsProfile -Action "Add" -Profile $Profile -Account $Account
```

Understanding how recommendations are prioritized

Every recommendation made is given a weighting value that identifies the relative importance of the recommendation. Only the ten most important recommendations are shown.

How weights are calculated

Weightings are aggregate values based on three key factors:

- The *probability* that an issue identified will cause problems. A higher probability equates to a larger overall score for the recommendation.
- The *impact* of the issue on your organization if it does cause a problem. A higher impact equates to a larger overall score for the recommendation.
- The *effort* required to implement the recommendation. A higher effort equates to a smaller overall score for the recommendation.

The weighting for each recommendation is expressed as a percentage of the total score available for each focus area. For example, if a recommendation in the Security and Compliance focus area has a score of 5%, implementing that recommendation will increase your overall Security and Compliance score by 5%.

Focus areas

Security and Compliance - This focus area shows recommendations for potential security threats and breaches, corporate policies, and technical, legal and regulatory compliance requirements.

Availability and Business Continuity - This focus area shows recommendations for service availability, resiliency of your infrastructure, and business protection.

Performance and Scalability - This focus area shows recommendations to help your organization's IT infrastructure grow, ensure that your IT environment meets current performance requirements, and is able to respond to changing infrastructure needs.

Upgrade, Migration and Deployment - This focus area shows recommendations to help you upgrade, migrate, and deploy SQL Server to your existing infrastructure.

Operations and Monitoring - This focus area shows recommendations to help streamline your IT operations, implement preventative maintenance, and maximize performance.

Change and Configuration Management - This focus area shows recommendations to help protect day-to-day operations, ensure that changes don't negatively affect your infrastructure, establish change control procedures, and to track and audit system configurations.

Should you aim to score 100% in every focus area?

Not necessarily. The recommendations are based on the knowledge and experiences gained by Microsoft engineers across thousands of customer visits. However, no two server infrastructures are the same, and specific recommendations may be more or less relevant to you. For example, some security recommendations might be less relevant if your virtual machines are not exposed to the Internet. Some availability recommendations may be less relevant for services that provide low priority ad hoc data collection and reporting. Issues that are important to a mature business may be less important to a start-up. You may want to identify which focus areas are your priorities and then look at how your scores change over time.

Every recommendation includes guidance about why it is important. You should use this guidance to evaluate whether implementing the recommendation is appropriate for you, given the nature of your IT services and the business needs of your organization.

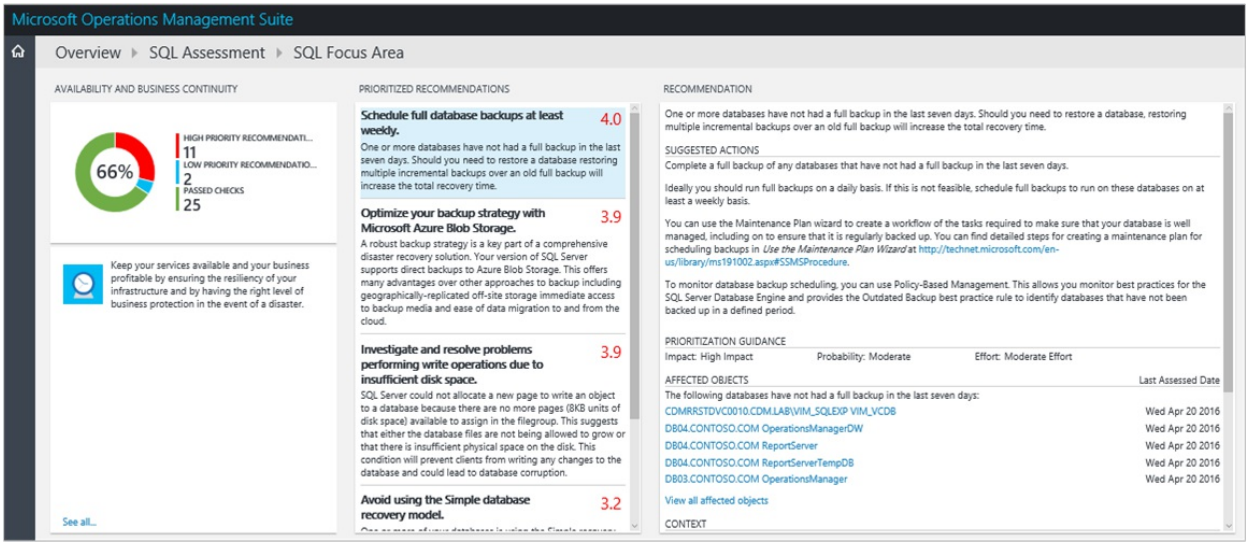
Use assessment focus area recommendations

Before you can use an assessment solution in OMS, you must have the solution installed. To read more about installing solutions, see Add Log Analytics solutions from the Solutions Gallery. After it is installed, you can view the summary of recommendations by using the SQL Assessment tile on the Overview page in OMS.

View the summarized compliance assessments for your infrastructure and then drill-into recommendations.

To view recommendations for a focus area and take corrective action

1. On the **Overview** page, click the **SQL Assessment** tile.
2. On the **SQL Assessment** page, review the summary information in one of the focus area blades and then click one to view recommendations for that focus area.
3. On any of the focus area pages, you can view the prioritized recommendations made for your environment. Click a recommendation under **Affected Objects** to view details about why the recommendation is made.



4. You can take corrective actions suggested in **Suggested Actions**. When the item has been addressed, later assessments will record that recommended actions were taken and your compliance score will increase. Corrected items appear as **Passed Objects**.

Ignore recommendations

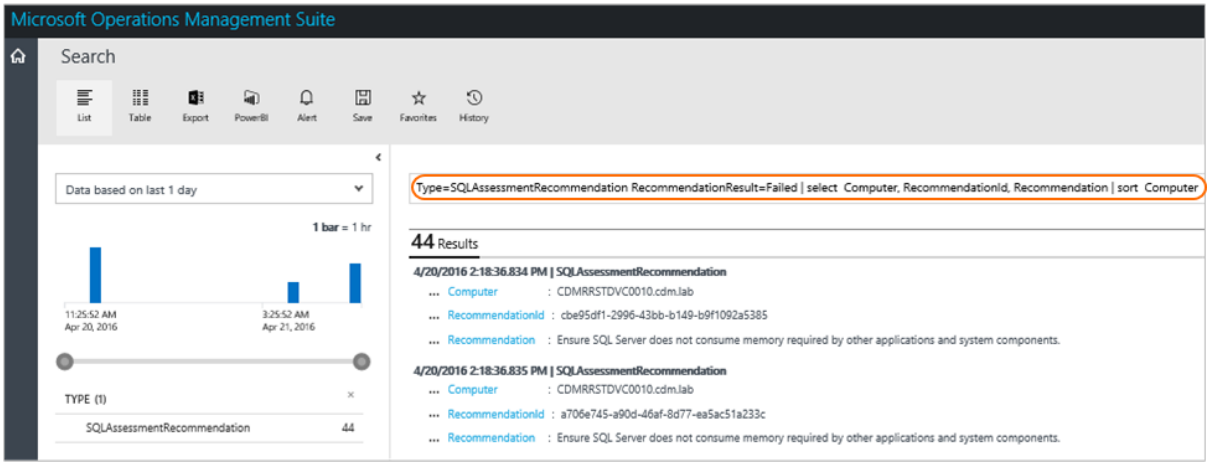
If you have recommendations that you want to ignore, you can create a text file that OMS will use to prevent recommendations from appearing in your assessment results.

To identify recommendations that you will ignore

1. Sign in to your workspace and open Log Search. Use the following query to list recommendations that have failed for computers in your environment.

```
Type=SQLAssessmentRecommendation RecommendationResult=Failed | select  Computer, RecommendationId, Recommendation | sort  Computer
```

Here's a screen shot showing the Log Search query:



2. Choose recommendations that you want to ignore. You'll use the values for RecommendationId in the next

procedure.

To create and use an IgnoreRecommendations.txt text file

1. Create a file named IgnoreRecommendations.txt.
2. Paste or type each RecommendationId for each recommendation that you want OMS to ignore on a separate line and then save and close the file.
3. Put the file in the following folder on each computer where you want OMS to ignore recommendations.
   - On computers with the Microsoft Monitoring Agent (connected directly or through Operations Manager) - *SystemDrive*:\Program Files\Microsoft Monitoring Agent\Agent
   - On the Operations Manager management server - *SystemDrive*:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server

To verify that recommendations are ignored

1. After the next scheduled assessment runs, by default every 7 days, the specified recommendations are marked Ignored and will not appear on the assessment dashboard.
2. You can use the following Log Search queries to list all the ignored recommendations.

```
Type=SQLAssessmentRecommendation RecommendationResult=Ignored | select  Computer, RecommendationId,
Recommendation | sort  Computer
```

3. If you decide later that you want to see ignored recommendations, remove any IgnoreRecommendations.txt files, or you can remove RecommendationIDs from them.

SQL Assessment solution FAQ

How often does an assessment run?

- The assessment runs every 7 days.

Is there a way to configure how often the assessment runs?

- Not at this time.

If another server is discovered after I've added the SQL assessment solution, will it be assessed?

- Yes, once it is discovered it is assessed from then on, every 7 days.

If a server is decommissioned, when will it be removed from the assessment?

- If a server does not submit data for 3 weeks, it is removed.

What is the name of the process that does the data collection?

- AdvisorAssessment.exe

How long does it take for data to be collected?

- The actual data collection on the server takes about 1 hour. It may take longer on servers that have a large number of SQL instances or databases.

What type of data is collected?

- The following types of data are collected:
  - WMI
  - Registry
  - Performance counters
  - SQL dynamic management views (DMV).

Is there a way to configure when data is collected?

- Not at this time.

Why do I have to configure a Run As Account?

- For SQL Server, a small number of SQL queries are run. In order for them to run, a Run As Account with VIEW SERVER STATE permissions to SQL must be used. In addition, in order to query WMI, local administrator credentials are required.

Why display only the top 10 recommendations?

- Instead of giving you an exhaustive overwhelming list of tasks, we recommend that you focus on addressing the prioritized recommendations first. After you address them, additional recommendations will become available. If you prefer to see the detailed list, you can view all recommendations using the OMS log search.

Is there a way to ignore a recommendation?

- Yes, see Ignore recommendations section above.

Next steps

- Search logs to view detailed SQL Assessment data and recommendations.

Monitor Surface Hubs with Log Analytics to track their health

4/12/2017 • 3 min to read • Edit Online

This article describes how you can use the Surface Hub solution in Log Analytics to monitor Microsoft Surface Hub devices with the Microsoft Operations Management Suite (OMS). Log Analytics helps you track the health of your Surface Hubs as well as understand how they are being used.

Each Surface Hub has the Microsoft Monitoring Agent installed. Its through the agent that you can send data from your Surface Hub to OMS. Log files are read from your Surface Hubs and are then are sent to the OMS service. Issues like servers being offline, the calendar not syncing, or if the device account is unable to log into Skype are shown in OMS in the Surface Hub dashboard. By using the data in the dashboard, you can identify devices that are not running, or that are having other problems, and potentially apply fixes for the detected issues.

Installing and configuring the solution

Use the following information to install and configure the solution. In order to manage your Surface Hubs from the Microsoft Operations Management Suite (OMS), you'll need the following:

- A valid subscription to OMS.
- An OMS subscription level that will support the number of devices you want to monitor. OMS pricing varies depending on how many devices are enrolled, and how much data it processes. You'll want to take this into consideration when planning your Surface Hub rollout.

Next, you will either add an OMS subscription to your existing Microsoft Azure subscription or create a new workspace directly through the OMS portal. Detailed instructions for using either method is at Get started with Log Analytics. Once the OMS subscription is set up, there are two ways to enroll your Surface Hub devices:

- Automatically through InTune
- Manually through **Settings** on your Surface Hub device.

Set up monitoring

You can monitor the health and activity of your Surface Hub using Log Analytics in OMS. You can enroll the Surface Hub in OMS by using InTune, or locally by using **Settings** on the Surface Hub.

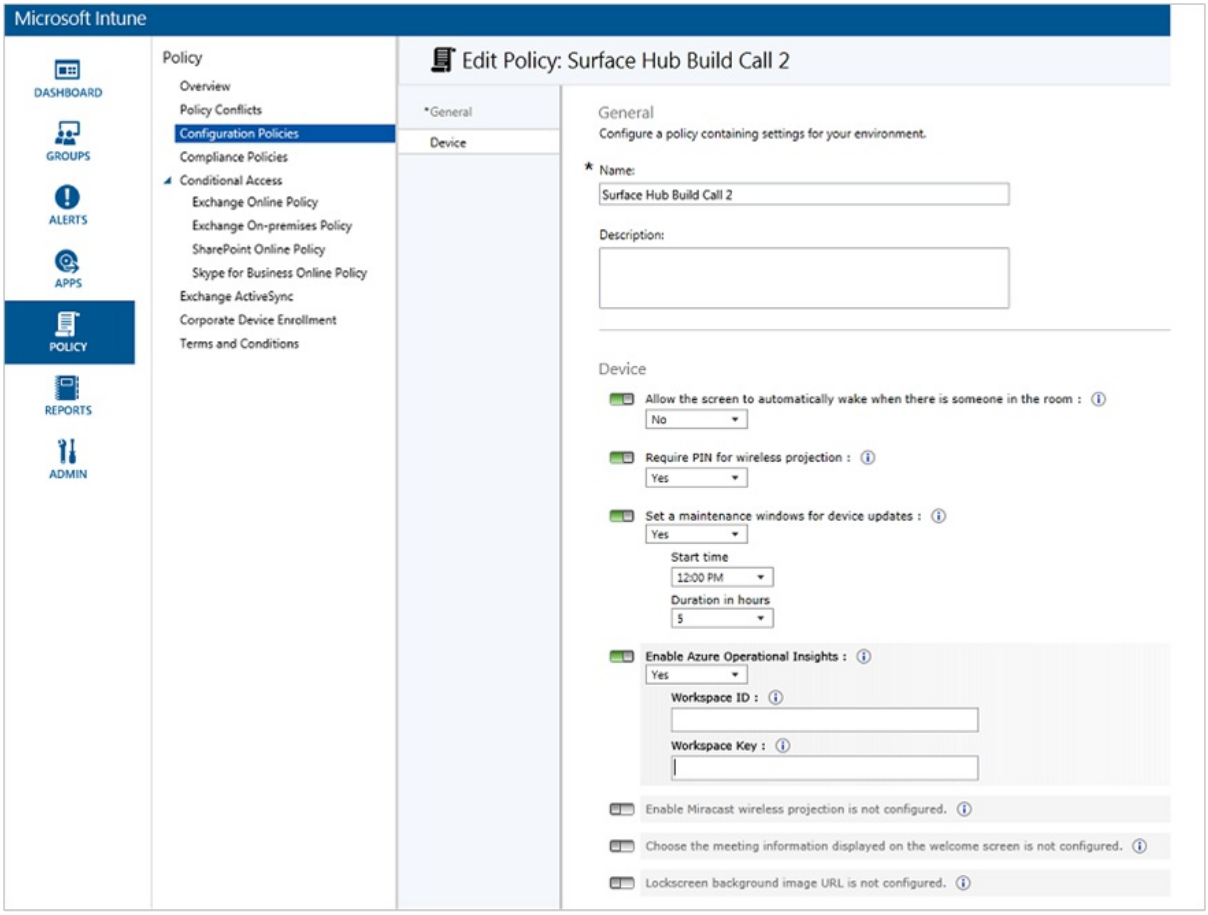
Connect Surface Hubs to OMS through InTune

You'll need the workspace ID and workspace key for the OMS workspace that will manage your Surface Hubs. You can get those from the OMS portal.

InTune is a Microsoft product that allows you to centrally manage the OMS configuration settings that are applied to one or more of your devices. Follow these steps to configure your devices through InTune:

1. Sign in to InTune.
2. Navigate to **Settings** > **Connected Sources**.
3. Create or edit a policy based on the Surface Hub template.
4. Navigate to the OMS (Azure Operational Insights) section of the policy, and add the *Workspace ID* and *Workspace Key* to the policy.
5. Save the policy.

6. Associate the policy with the appropriate group of devices.



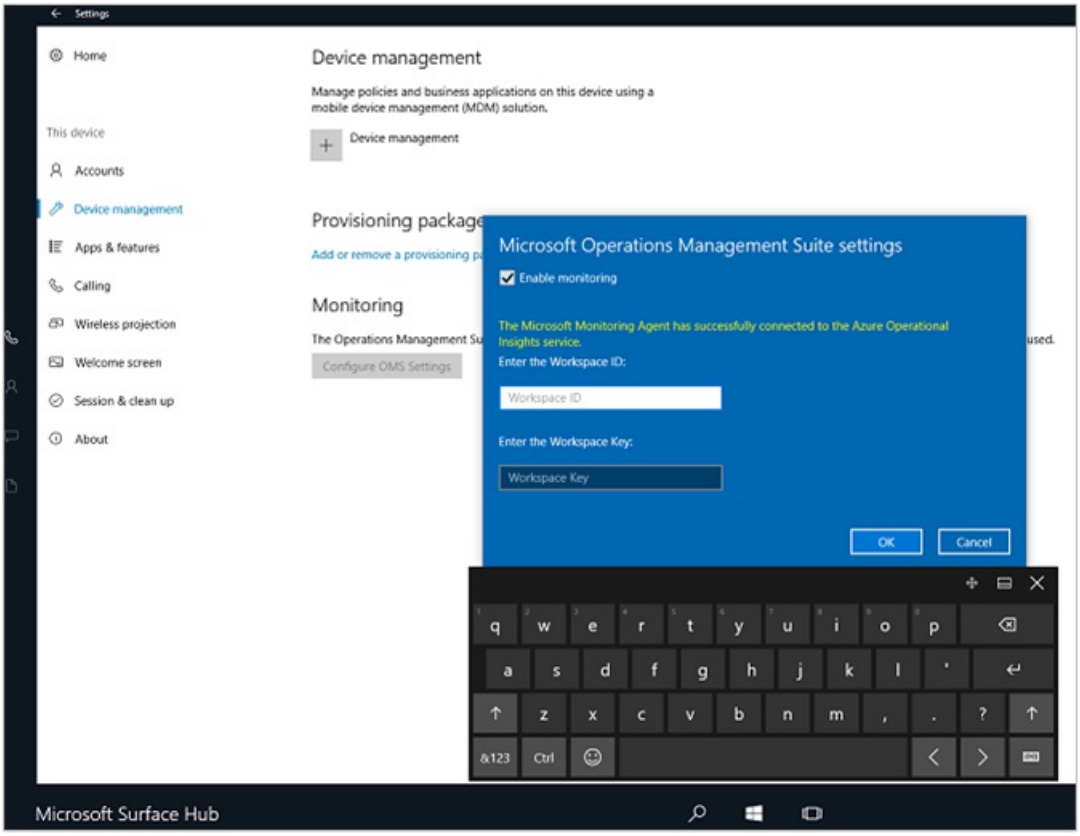
InTune then syncs the OMS settings with the devices in the target group, enrolling them in your OMS workspace.

Connect Surface Hubs to OMS using the Settings app

You'll need the workspace ID and workspace key for the OMS workspace that will manage your Surface Hubs. You can get those from the OMS portal.

If you don't use InTune to manage your environment, you can enroll devices manually through **Settings** on each Surface Hub:

1. From your Surface Hub, open **Settings**.
2. Enter the device admin credentials when prompted.
3. Click **This device**, and the under **Monitoring**, click **Configure OMS Settings**.
4. Select **Enable monitoring**.
5. In the OMS settings dialog, type the **Workspace ID** and type the **Workspace Key**.



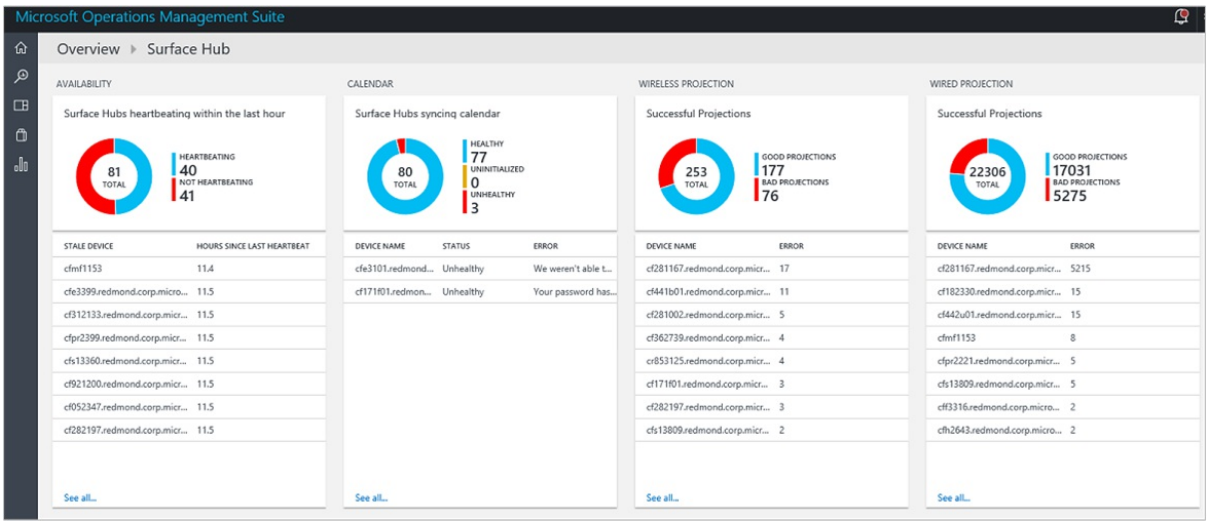
6. Click **OK** to complete the configuration.

A confirmation appears telling you whether or not the OMS configuration was successfully applied to the device. If it was, a message appears stating that the agent successfully connected to the OMS service. The device then starts sending data to OMS where you can view and act on it.

Monitor Surface Hubs

Monitoring your Surface Hubs using OMS is much like monitoring any other enrolled devices.

1. Sign in to the OMS portal.
2. Navigate to the Surface Hub solution pack dashboard.
3. Your device's health is displayed.



You can create alerts based on existing or custom log searches. Using the data the OMS collects from your Surface Hubs, you can search for issues and alert on the conditions that you define for your devices.

Next steps

- Use Log searches in Log Analytics to view detailed Surface Hub data.
- Create alerts to notify you when issues occur with your Surface Hubs.

VMware Monitoring (Preview) solution in Log Analytics

4/12/2017 • 8 min to read • Edit Online

The VMware Monitoring solution in Log Analytics is a solution that helps you create a centralized logging and monitoring approach for large VMware logs. This article describes how you can troubleshoot, capture, and manage the ESXi hosts in a single location using the solution. With the solution, you can see detailed data for all your ESXi hosts in a single location. You can see top event counts, status, and trends of VM and ESXi hosts provided through the ESXi host logs. You can troubleshoot by viewing and searching centralized ESXi host logs. And, you can create alerts based on log search queries.

The solution uses native syslog functionality of the ESXi host to push data to a target VM, which has OMS Agent. However, the solution doesn't write files into syslog within the target VM. The OMS agent opens port 1514 and listens to this. Once it receives the data, the OMS agent pushes the data into OMS.

Installing and configuring the solution

Use the following information to install and configure the solution.

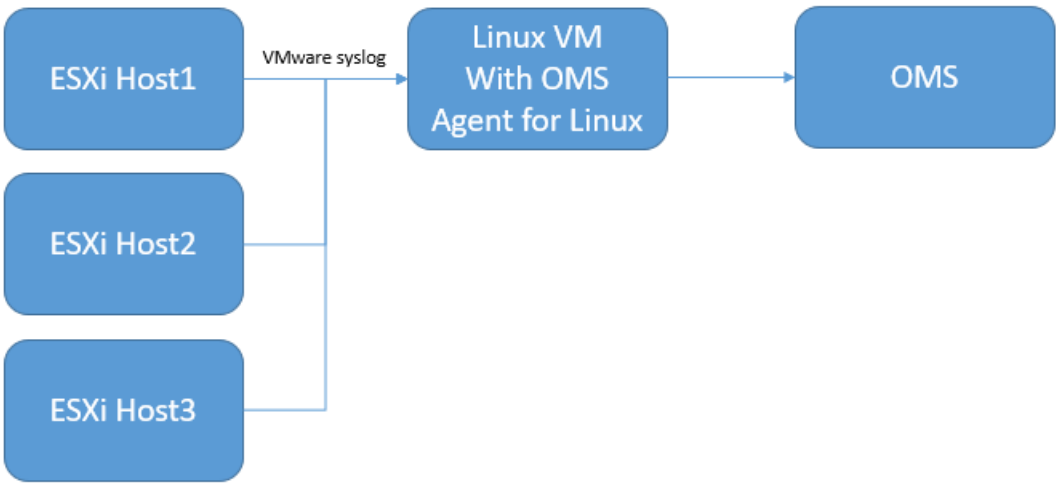
- Add the VMware Monitoring solution to your OMS workspace using the process described in Add Log Analytics solutions from the Solutions Gallery.

Supported VMware ESXi hosts

vSphere ESXi Host 5.5 and 6.0

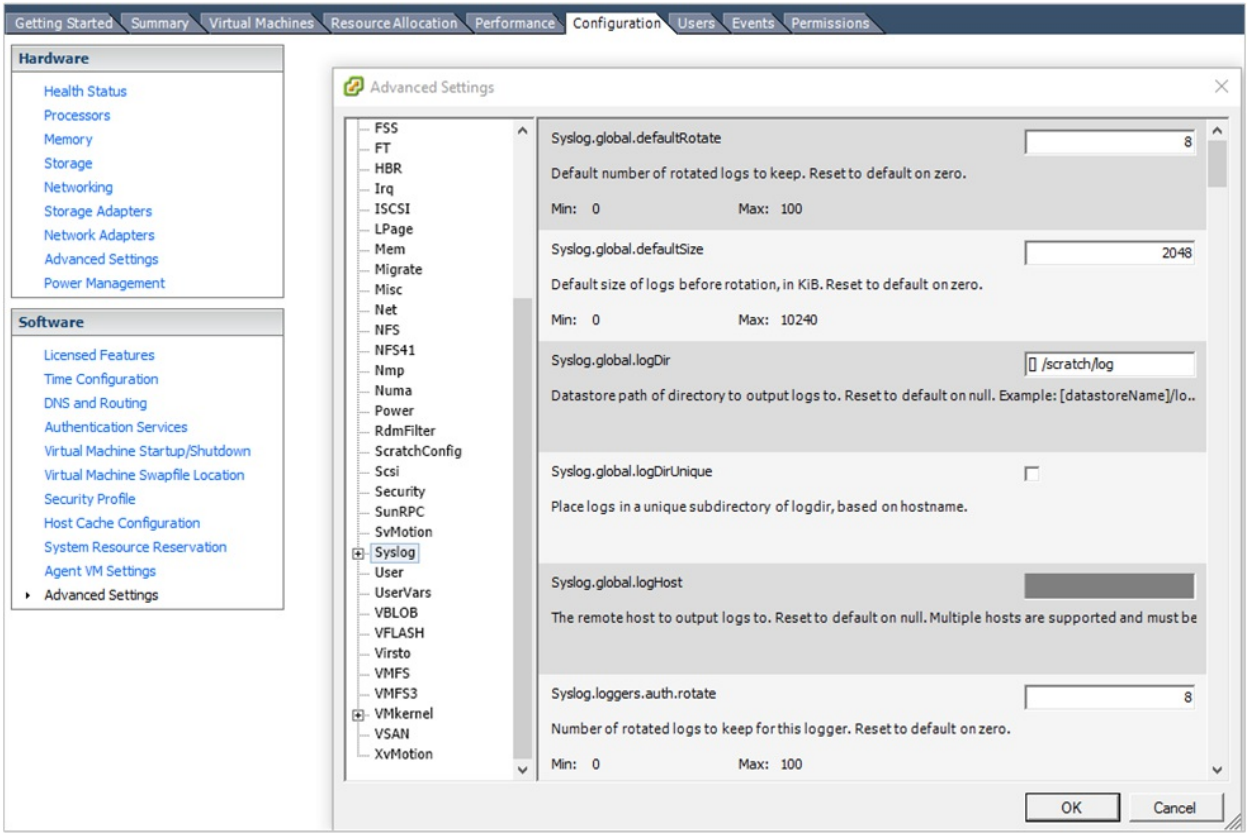
Prepare a Linux server

Create a Linux operating system VM to receive all syslog data from the ESXi hosts. The OMS Linux Agent is the collection point for all ESXi host syslog data. You can use multiple ESXi hosts to forward logs to a single Linux server, as in the following example.

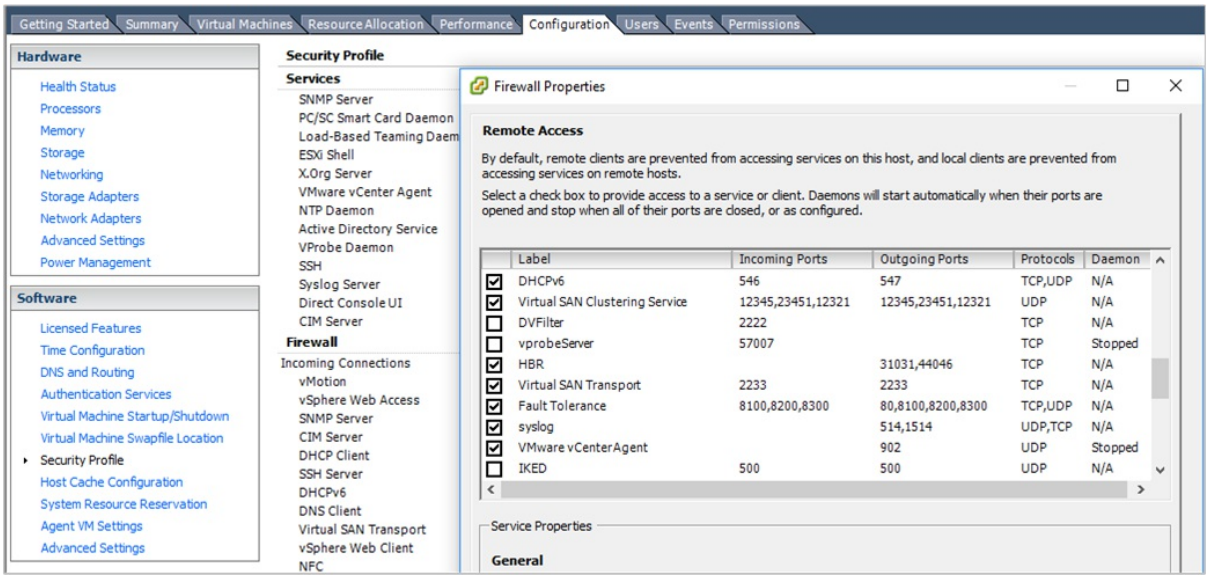


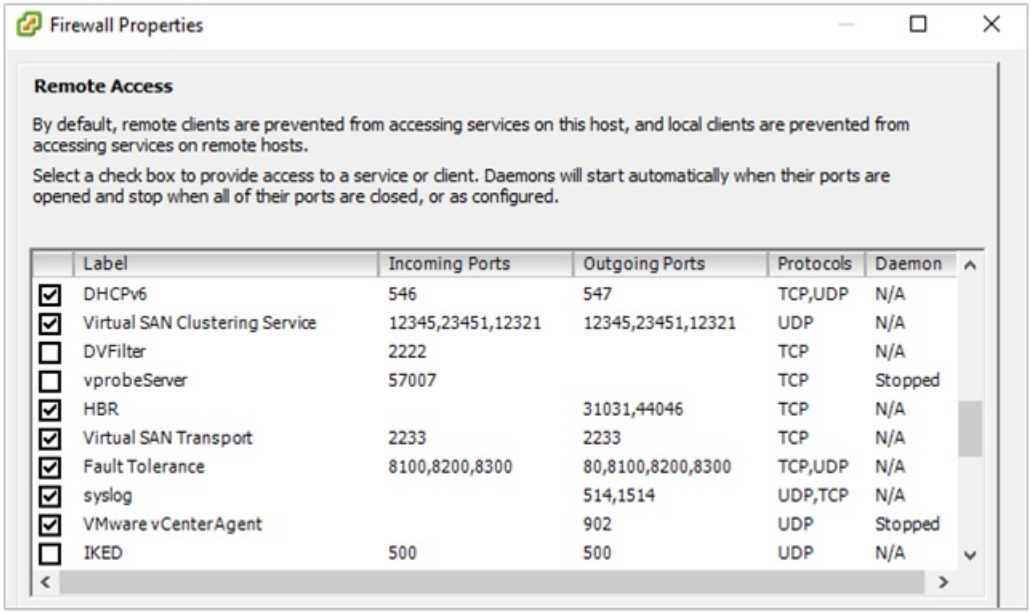
Configure syslog collection

1. Set up syslog forwarding for VSphere. For detailed information to help set up syslog forwarding, see Configuring syslog on ESXi 5.x and 6.0 (2003322). Go to **ESXi Host Configuration** > **Software** > **Advanced Settings** > **Syslog**.



2. In the *Syslog.global.logHost* field, add your Linux server and the port number *1514*. For example, `tcp://hostname:1514` or `tcp://123.456.789.101:1514`
3. Open the ESXi host firewall for syslog. **ESXi Host Configuration** > **Software** > **Security Profile** > **Firewall** and open **Properties**.





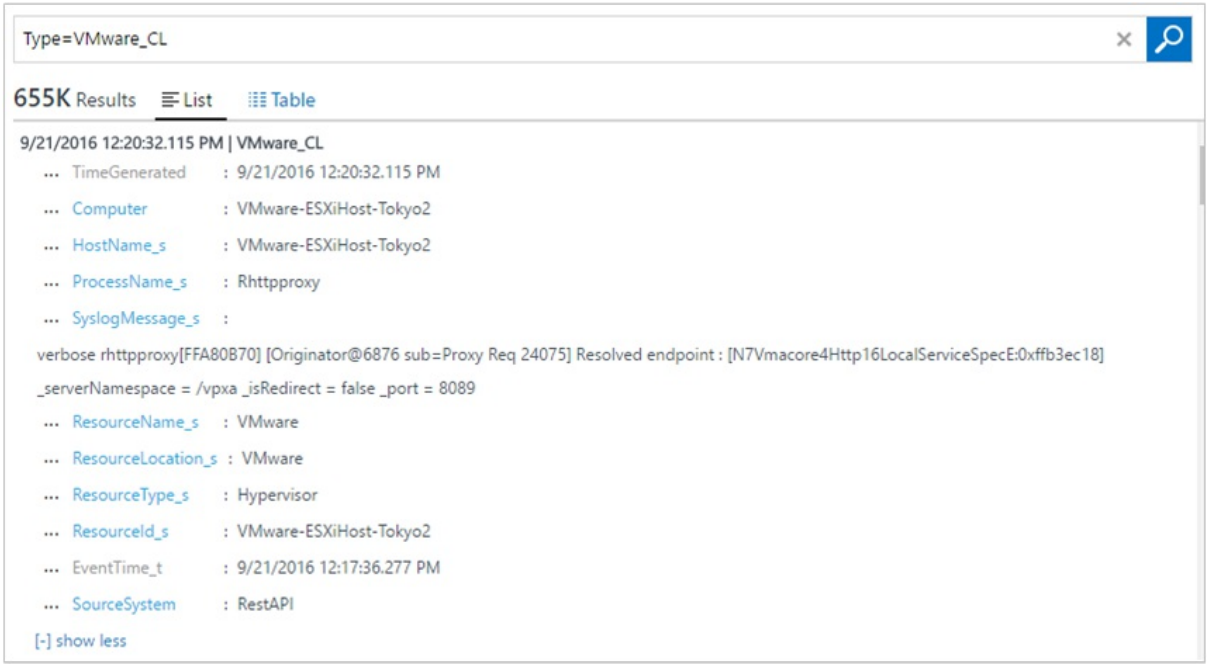
4. Check the vSphere Console to verify that that syslog is properly set up. Confirm on the ESXI host that port **1514** is configured.
5. Download and install the OMS Agent for Linux on the Linux server. For more information, see the Documentation for OMS Agent for Linux.
6. After the OMS Agent for Linux is installed, go to the /etc/opt/microsoft/omsagent/sysconf/omsagent.d directory and copy the vmware_esxi.conf file to the /etc/opt/microsoft/omsagent/conf/omsagent.d directory and the change the owner/group and permissions of the file. For example:

```
sudo cp /etc/opt/microsoft/omsagent/sysconf/omsagent.d/vmware_esxi.conf
/etc/opt/microsoft/omsagent/conf/omsagent.d
sudo chown omsagent:omiusers /etc/opt/microsoft/omsagent/conf/omsagent.d/vmware_esxi.conf
```

7. Restart the OMS Agent for Linux by running `sudo /opt/microsoft/omsagent/bin/service_control restart`.
8. Test the connectivity between the Linux server and the ESXi host by using the `nc` command on the ESXi Host. For example:

```
[root@ESXiHost:~] nc -z 123.456.789.101 1514
Connection to 123.456.789.101 1514 port [tcp/*] succeeded!
```

9. In the OMS Portal, perform a log search for `Type=VMware_CL`. When OMS collects the syslog data, it retains the syslog format. In the portal, some specific fields are captured, such as *Hostname* and *ProcessName*.



If your view log search results are similar to the image above, you're set to use the OMS VMware Monitoring solution dashboard.

VMware data collection details

The VMware Monitoring solution collects various performance metrics and log data from ESXi hosts using the OMS Agents for Linux that you have enabled.

The following table shows data collection methods and other details about how data is collected.

PLATFORM	OMS AGENT FOR LINUX	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Linux						every 3 minutes

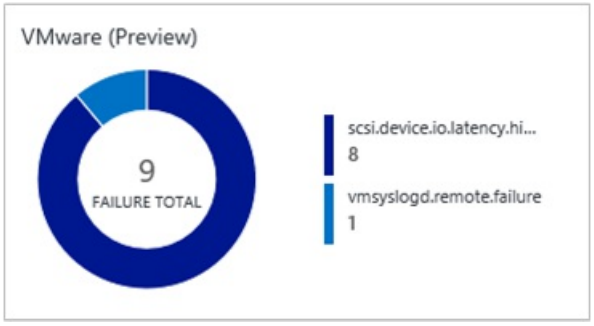
The following table show examples of data fields collected by the VMware Monitoring solution:

FIELD NAME	DESCRIPTION
Device_s	VMware storage devices
ESXIFailure_s	failure types
EventTime_t	time when event occurred
HostName_s	ESXi host name
Operation_s	create VM or delete VM
ProcessName_s	event name
ResourceId_s	name of the VMware host
ResourceLocation_s	VMware

FIELD NAME	DESCRIPTION
ResourceName_s	VMware
ResourceType_s	Hyper-V
SCSIStatus_s	VMware SCSI status
SyslogMessage_s	Syslog data
UserName_s	user who created or deleted VM
VMName_s	VM name
Computer	host computer
TimeGenerated	time the data was generated
DataCenter_s	VMware datacenter
StorageLatency_s	storage latency (ms)

VMware Monitoring solution overview

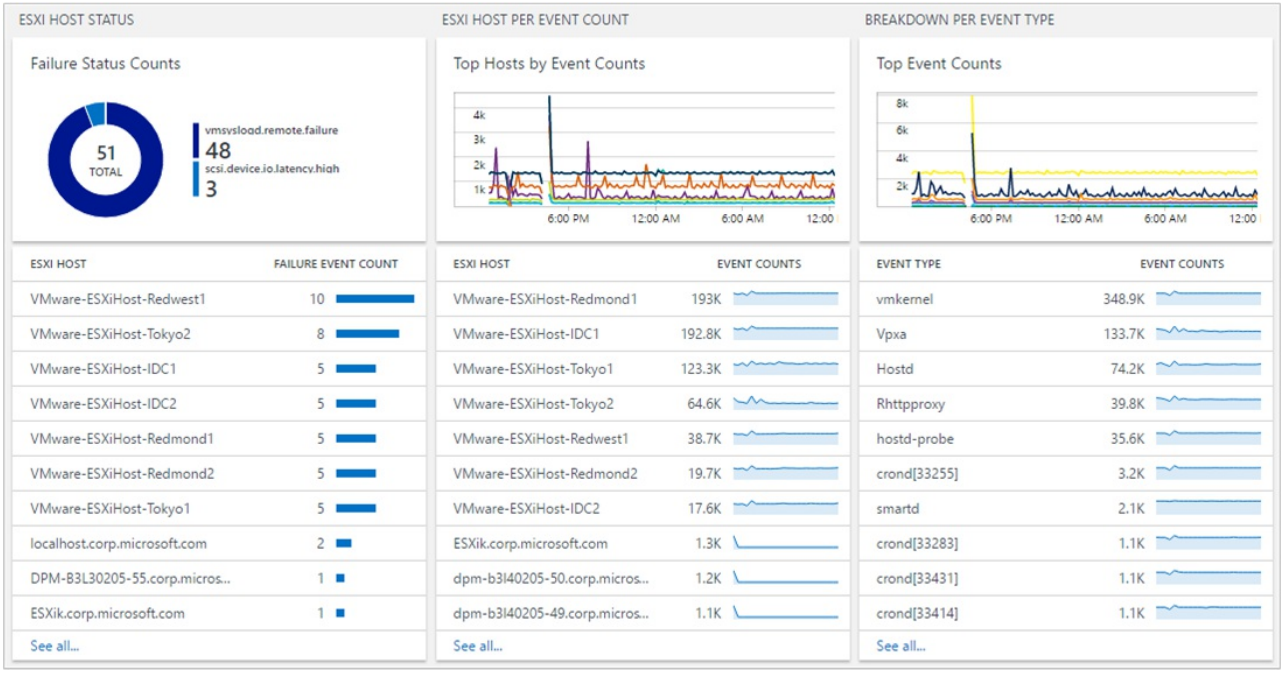
The VMware tile appears in the OMS portal. It provides a high-level view of any failures. When you click the tile, you go into a dashboard view.



Navigate the dashboard view

In the **VMware** dashboard view, blades are organized by:

- Failure Status Count
- Top Host by Event Counts
- Top Event Counts
- Virtual Machine Activities
- ESXi Host Disk Events

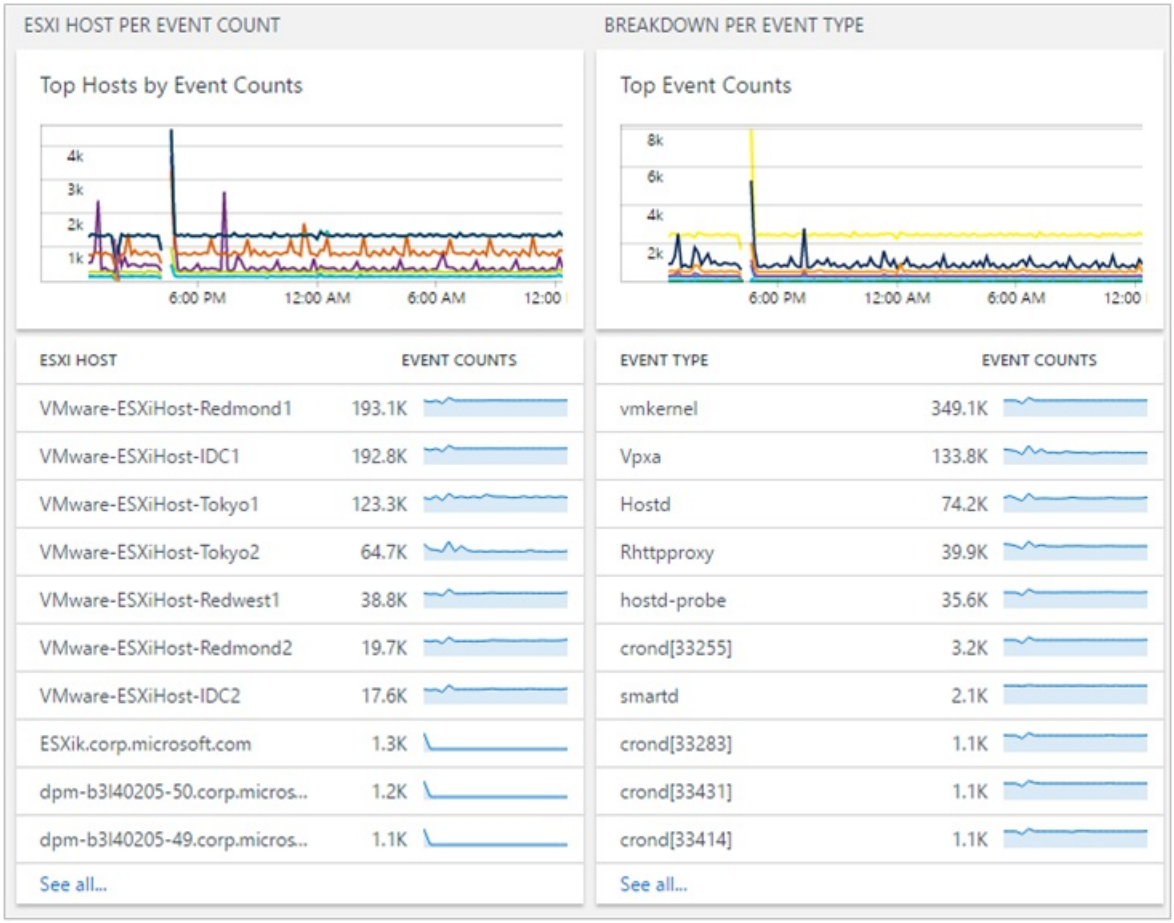


Click any blade to open Log Analytics search pane that shows detailed information specific for the blade.

From here, you can edit the search query to modify it for something specific. For a tutorial on the basics of OMS search, check out the OMS log search tutorial.

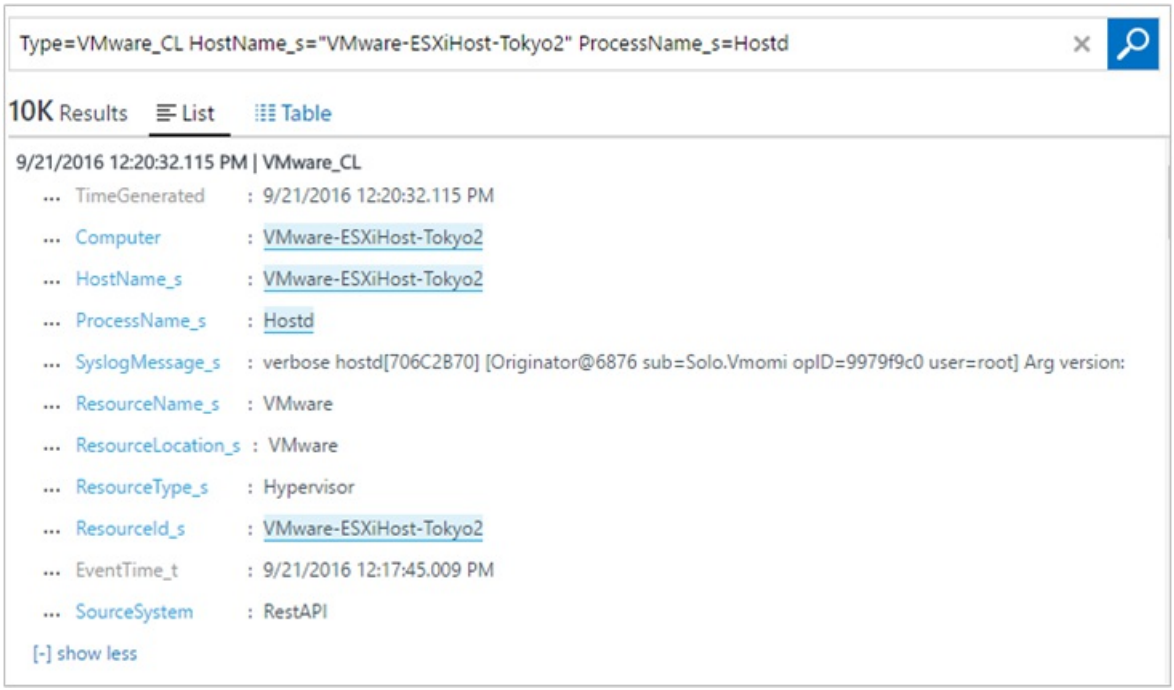
Find ESXi host events

A single ESXi host generates multiple logs, based on their processes. The VMware Monitoring solution centralizes them and summarizes the event counts. This centralized view helps you understand which ESXi host has a high volume of events and what events occur most frequently in your environment.



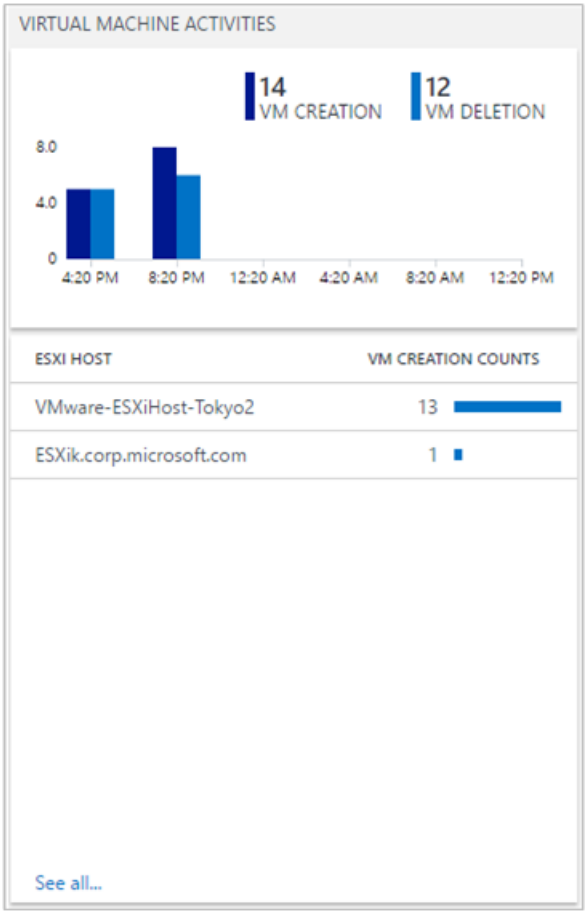
You can drill further by clicking an ESXi host or an event type.

When you click an ESXi host name, you view information from that ESXi host. If you want to narrow results with the event type, add `"ProcessName_s=EVENT TYPE"` in your search query. You can select **ProcessName** in the search filter. That narrows the information for you.

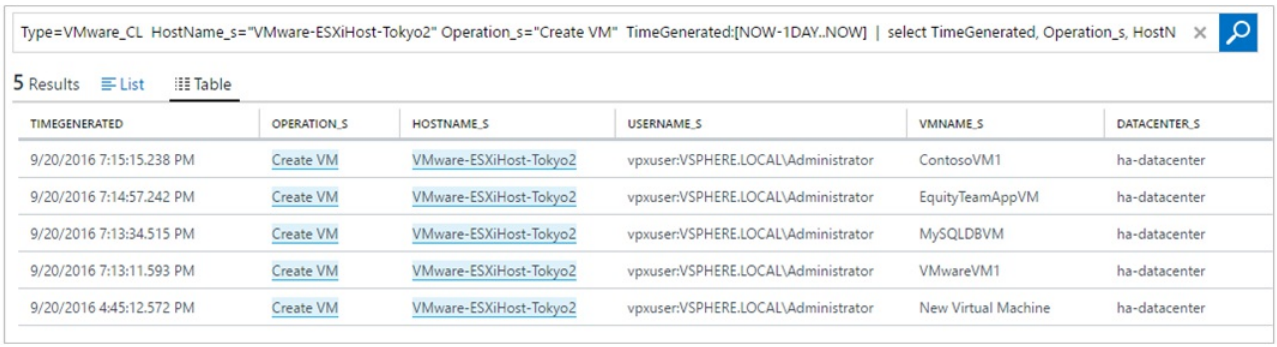


Find high VM activities

A virtual machine can be created and deleted on any ESXi host. It's helpful for an administrator to identify how many VMs an ESXi host creates. That in-turn, helps to understand performance and capacity planning. Keeping track of VM activity events is crucial when managing your environment.



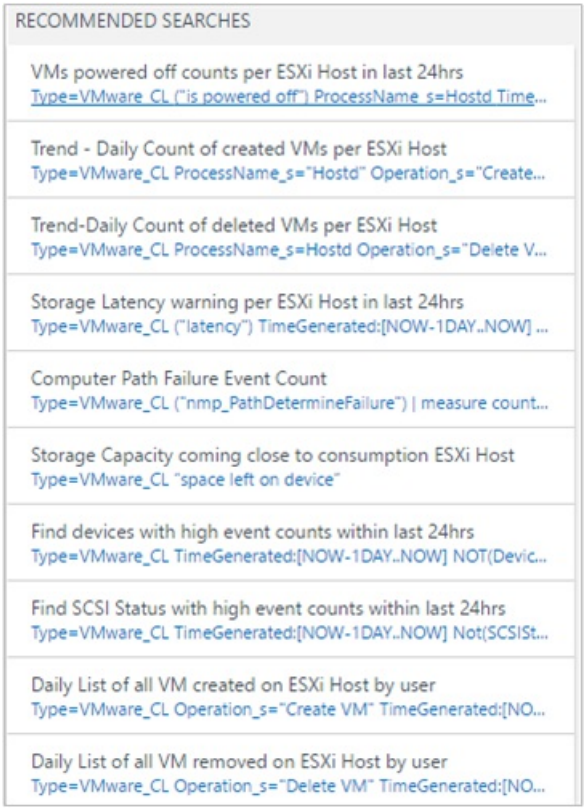
If you want to see additional ESXi host VM creation data, click an ESXi host name.



TIMEGENERATED	OPERATION_S	HOSTNAME_S	USERNAME_S	VMNAME_S	DATACENTER_S
9/20/2016 7:15:15.238 PM	Create VM	VMware-ESXiHost-Tokyo2	vpxuser:VSPHERE.LOCAL\Administrator	ContosoVM1	ha-datacenter
9/20/2016 7:14:57.242 PM	Create VM	VMware-ESXiHost-Tokyo2	vpxuser:VSPHERE.LOCAL\Administrator	EquityTeamAppVM	ha-datacenter
9/20/2016 7:13:34.515 PM	Create VM	VMware-ESXiHost-Tokyo2	vpxuser:VSPHERE.LOCAL\Administrator	MySQLDBVM	ha-datacenter
9/20/2016 7:13:11.593 PM	Create VM	VMware-ESXiHost-Tokyo2	vpxuser:VSPHERE.LOCAL\Administrator	VMwareVM1	ha-datacenter
9/20/2016 4:45:12.572 PM	Create VM	VMware-ESXiHost-Tokyo2	vpxuser:VSPHERE.LOCAL\Administrator	New Virtual Machine	ha-datacenter

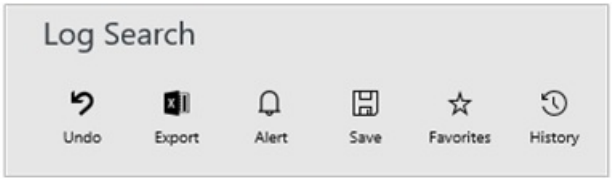
Common search queries

The solution includes other useful queries that can help you manage your ESXi hosts, such as high storage space, storage latency, and path failure.



Save queries

Saving search queries is a standard feature in OMS and can help you keep any queries that you've found useful. After you create a query that you find useful, save it by clicking the **Favorites**. A saved query lets you easily reuse it later from the My Dashboard page where you can create your own custom dashboards.



Create alerts from queries

After you've created your queries, you might want to use the queries to alert you when specific events occur. See Alerts in Log Analytics for information about how to create alerts. For examples of alerting queries and other query examples, see the Monitor VMware using OMS Log Analytics blog post.

Frequently asked questions

What do I need to do on the ESXi host setting? What impact will it have on my current environment?

The solution uses the native ESXi Host Syslog forwarding mechanism. You don't need any additional Microsoft software on the ESXi Host to capture the logs. It should have a low impact to your existing environment. However, you do need to set syslog forwarding, which is ESXI functionality.

Do I need to restart my ESXi host?

No. This process does not require a restart. Sometimes, vSphere does not properly update the syslog. In such a case, log on to the ESXi host and reload the syslog. Again, you don't have to restart the host, so this process isn't disruptive to your environment.

Can I increase or decrease the volume of log data sent to OMS?

Yes you can. You can use the ESXi Host Log Level settings in vSphere. Log collection is based on the *info* level. So, if you want to audit VM creation or deletion, you need to keep the *info* level on Hostd. For more information, see the VMware Knowledge Base.

Why is Hostd not providing data to OMS? My log setting is set to info.

There was an ESXi host bug for the syslog timestamp. For more information, see the VMware Knowledge Base. After you apply the workaround, Hostd should function normally.

Can I have multiple ESXi hosts forwarding syslog data to a single VM with omsagent?

Yes. You can have multiple ESXi hosts forwarding to a single VM with omsagent.

Why don't I see data flowing into OMS?

There can be multiple reasons:

- The ESXi host is not correctly pushing data to the VM running omsagent. To test, perform the following steps:

  1. To confirm, log on to the ESXi host using ssh and run the following command:
     `nc -z ipaddressofVM 1514`

     If this is not successful, vSphere settings in the Advanced Configuration are likely not correct. See Configure syslog collection for information about how to set up the ESXi host for syslog forwarding.

  2. If syslog port connectivity is successful, but you don't still see any data, then reload the syslog on the ESXi host by using ssh to run the following command: `esxcli system syslog reload`

- The VM with OMS Agent is not set correctly. To test this, perform the following steps:

  1. OMS listens to the port 1514 and pushes data into OMS. To verify that it is open, run the following command: `netstat -a | grep 1514`
  2. You should see port `1514/tcp` open. If you do not, verify that the omsagent is installed correctly. If you do not see the port information, then the syslog port is not open on the VM.

     a. Verify that the OMS Agent is running by using `ps -ef | grep oms`. If it is not running, start the process by running the command `sudo /opt/microsoft/omsagent/bin/service_control start`

     b. Open the `/etc/opt/microsoft/omsagent/conf/omsagent.d/vmware_esxi.conf` file.

        Verify that the proper user and group setting is valid, similar to:
        `-rw-r--r-- 1 omsagent omiusers 677 Sep 20 16:46 vmware_esxi.conf`

        If the file does not exist or the user and group setting is wrong, take corrective action by Preparing a Linux server.

Next steps

- Use Log Searches in Log Analytics to view detailed VMware host data.
- Create your own dashboards showing VMware host data.
- Create alerts when specific VMware host events occur.

Wire Data solution in Log Analytics

4/5/2017 • 5 min to read • Edit Online

Wire data is consolidated network and performance data from computers with OMS agents, including Operations Manager and Windows-connected agents. Network data is combined with your log data to help you correlate data. OMS agents installed on computers in your IT infrastructure monitor network data sent to and from those computers for network levels 2-3 in the OSI model including the various protocols and ports used.

> **NOTE**
> The Wire Data 1.0 solution is not currently available to be added to workspaces. Customers who already have the Wire Data 1.0 solution enabled can continue to use the Wire Data 1.0 solution. New customers, however, should instead use the Wire Data 2.0 solution.

By default, OMS collects logged data for CPU, memory, disk, and network performance data from counters built into Windows. Network and other data collection is done in real-time for each agent, including subnets and application-level protocols being used by the computer. You can add other performance counters on the Settings page on the Logs tab.

If you've used sFlow or other software with Cisco's NetFlow protocol, then the statistics and data you'll see from wire data will be familiar to you.

Some of the types of built-in Log search queries include:

- Agents that provide wire data
- IP address of agents providing wire data
- Outbound communications by IP addresses
- Number of bytes sent by application protocols
- Number of bytes sent by an application service
- Bytes received by different protocols
- Total bytes sent and received by IP
- IP addresses that have communicated with agents on the 10.0.0.0/8 subnet
- Average latency for connections that were measured reliably
- Computer processes that initiated or received network traffic
- Amount of network traffic for a process

When you search using wire data, you can filter and group data to view information about the top agents and top protocols. Or you can look into when certain computers (IP addresses/MAC addresses) communicated with each other, for how long, and how much data was sent--basically, you view metadata about network traffic, which is search-based.

However, since you're viewing metadata, it's not necessarily useful for in-depth troubleshooting. Wire data in OMS is not a full capture of network data. So it's not intended for deep packet-level troubleshooting. The advantage of using the agent, compared to other collection methods, is that you don't have to install appliances, reconfigure your network switches, or preform complicated configurations. Wire data is simply agent-based--you install the agent on a computer and it will monitor its own network traffic. Another advantage is when you want to monitor workloads running in cloud providers or hosting service provider or Microsoft Azure, where the user doesn't own the fabric layer.

In contrast, you don't have complete visibility of what occurs on the network if you don't install agents on all the

computers in your network infrastructure.

Installing and configuring the solution

Use the following information to install and configure the solution.

- The Wire Data solution acquires data from computers running Windows Server 2012 R2, Windows 8.1, and later operating systems.
- Microsoft .NET Framework 4.0 or later is required on computers where you want to acquire wire data from.
- Add the Wire Data solution to your OMS workspace using the process described in Add Log Analytics solutions from the Solutions Gallery. There is no further configuration required.
- If you want to view wire data for a specific solution, you'll need to have the solution already added to your OMS workspace.

Wire Data data collection details

Wire data collects metadata about network traffic using the agents that you have enabled.

The following table shows data collection methods and other details about how data is collected for Wire Data.

PLATFORM	DIRECT AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows (2012 R2 / 8.1 or later)						every 1 minute

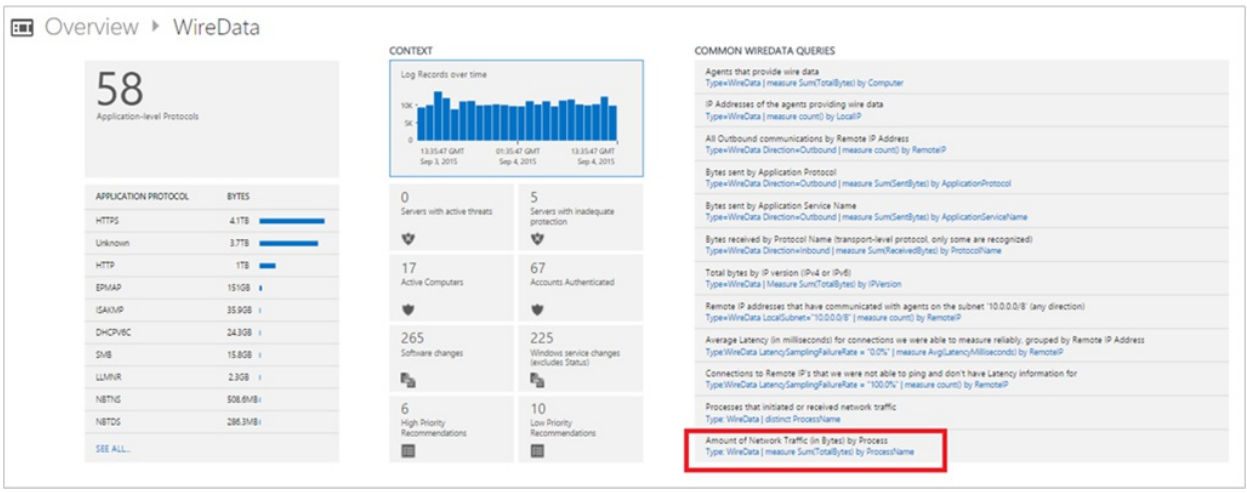
Combining wire data with other solution data

Data returned from the built-in queries shown above might be interesting by itself. However, the usefulness of wire data is realized when you combine it with information from other OMS solutions. For example, you can use security event data collected by the Security and Audit solution and combine it with wire data to look for unusual network logon attempts for named processes. In this example, you'd use the IN and DISTINCT operators to join data points in your search query.

Requirements: In order to use the following example, you'll need to have the Security and Audit solution installed. However, you can use data from other solutions to combine with wire data to achieve similar results.

To combine wire data with security events

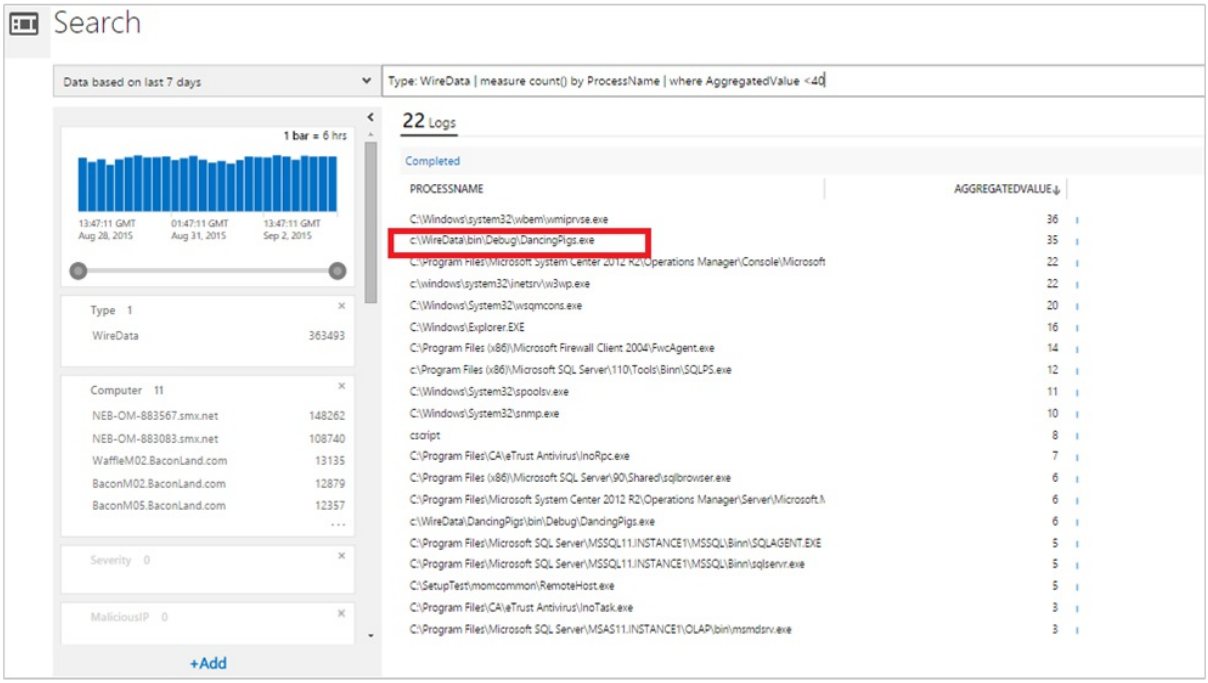
1. On the Overview page, click the **WireData** tile.
2. In the list of **Common WireData Queries**, click **Amount of Network Traffic (in Bytes) by Process** to see the list of returned processes.



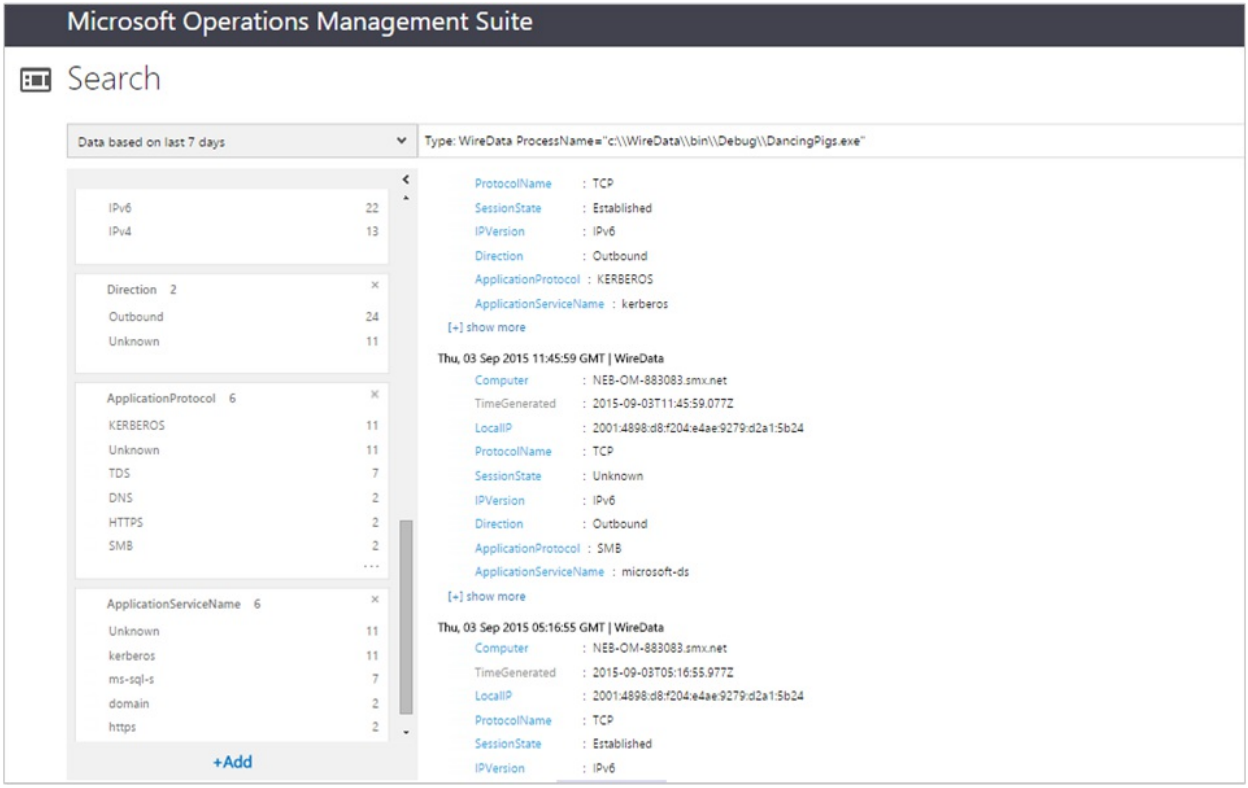
3. If the list of processes is too long to easily view, you can modify the search query to resemble:

```
Type WireData | measure count() by ProcessName | where AggregatedValue <40
```

Shown in the example below is a process named DancingPigs.exe, which might appear suspicious.

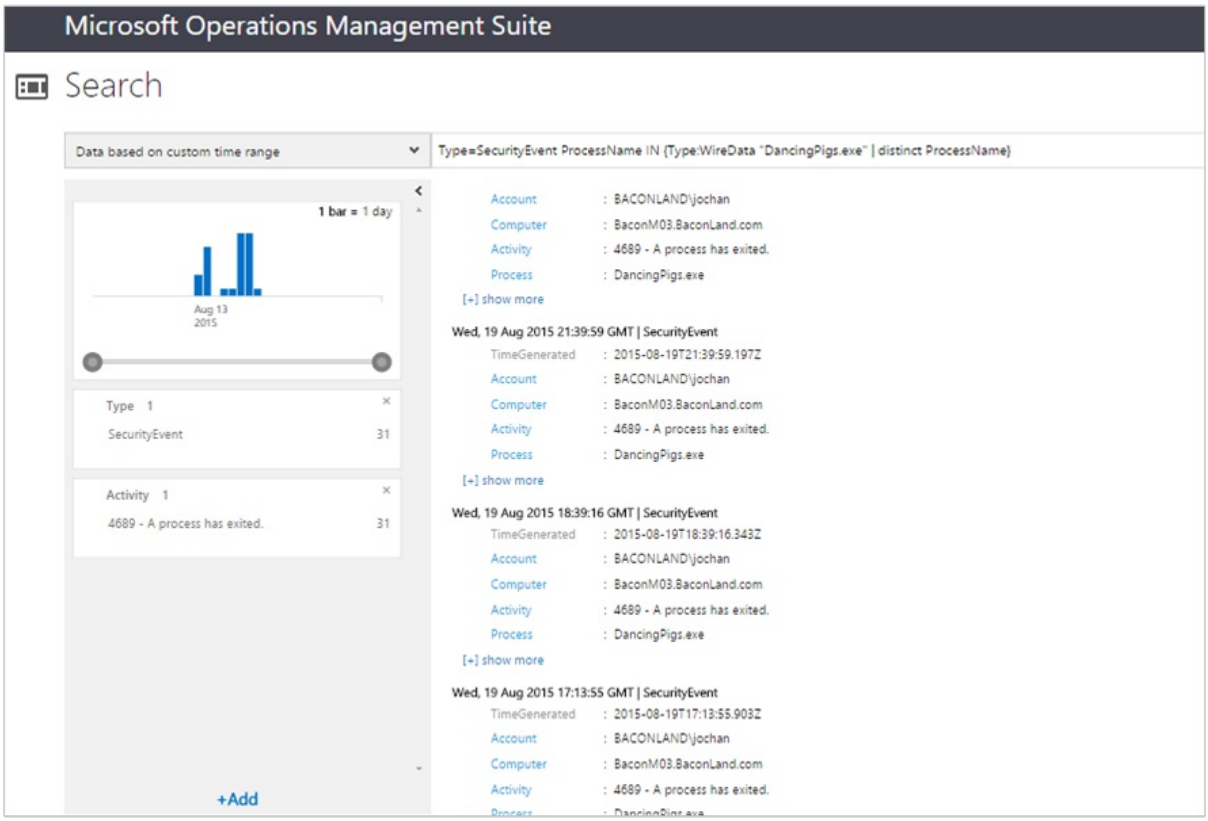


4. Using data returned in your list, click a named process. In this example, DancingPigs.exe was clicked. The results shown below describe the type of network traffic such as outbound communication over various protocols.



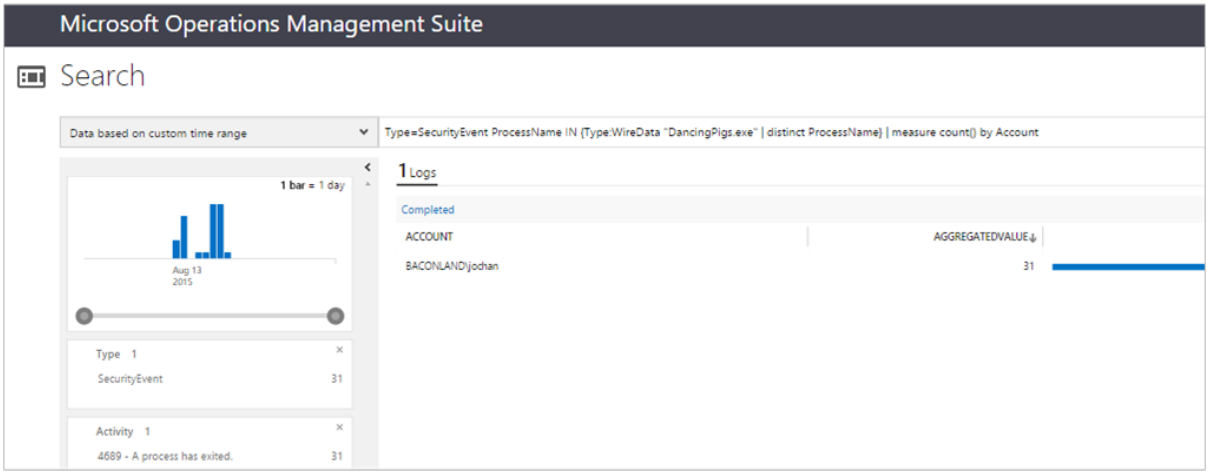
5. Because the Security and Audit solution is installed, you can probe into the security events that have the same ProcessName field value by modifying your search query using the IN and DISTINCT search query operators. You can do that then when both your wire data and other solution logs have values in the same format. Modify your search query to resemble:

```
Type=SecurityEvent ProcessName IN {Type:WireData "DancingPigs.exe" | distinct ProcessName}
```



6. In the results above, you'll see that account information is shown. Now you can refine your search query to find out how often the account, showing Security and Audit data, was used by the process with a query resembling:

```
Type=SecurityEvent ProcessName IN {Type:WireData "DancingPigs.exe" | distinct ProcessName} | measure
count() by Account
```



Next steps

- Search logs to view detailed wire data search records.
- See Dan's Using Wire Data in Operations Management Suite Log Search blog post has additional information about how often data is collected and how you can modify collection properties for Operations Manager agents.

Track software changes in your environment with the Change Tracking solution

4/12/2017 • 6 min to read • Edit Online

This article helps you use the Change Tracking solution in Log Analytics to easily identify changes in your environment. The solution tracks changes to Windows and Linux software, Windows files and registry keys, Windows services, and Linux daemons. Identifying configuration changes can help you pinpoint operational issues.

You install the solution to update the type of agent that you have installed. Changes to installed software, Windows services, and Linux daemons on the monitored servers are read and then the data is sent to the Log Analytics service in the cloud for processing. Logic is applied to the received data and the cloud service records the data. By using the information on the Change Tracking dashboard, you can easily see the changes that were made in your server infrastructure.

Installing and configuring the solution

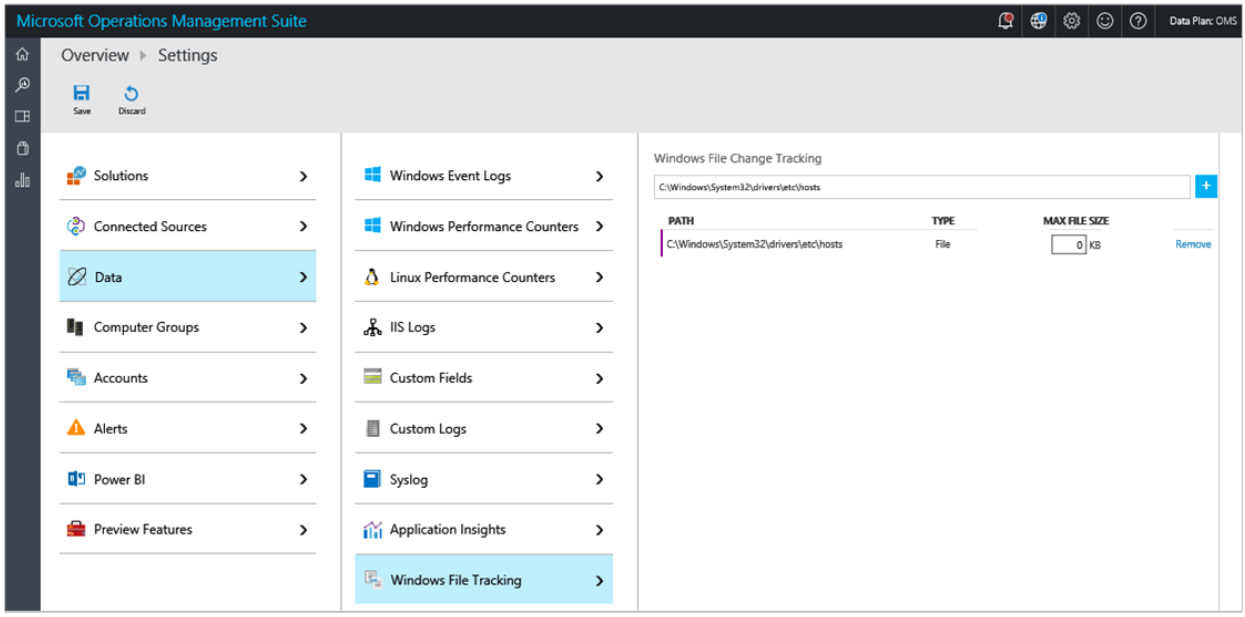
Use the following information to install and configure the solution.

- You must have a Windows, Operations Manager, or Linux agent on each computer where you want to monitor changes.
- Add the Change Tracking solution to your OMS workspace from the Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery. There is no further configuration required.

Configure Windows files to track

Use the following steps to configure files to track on Windows computers.

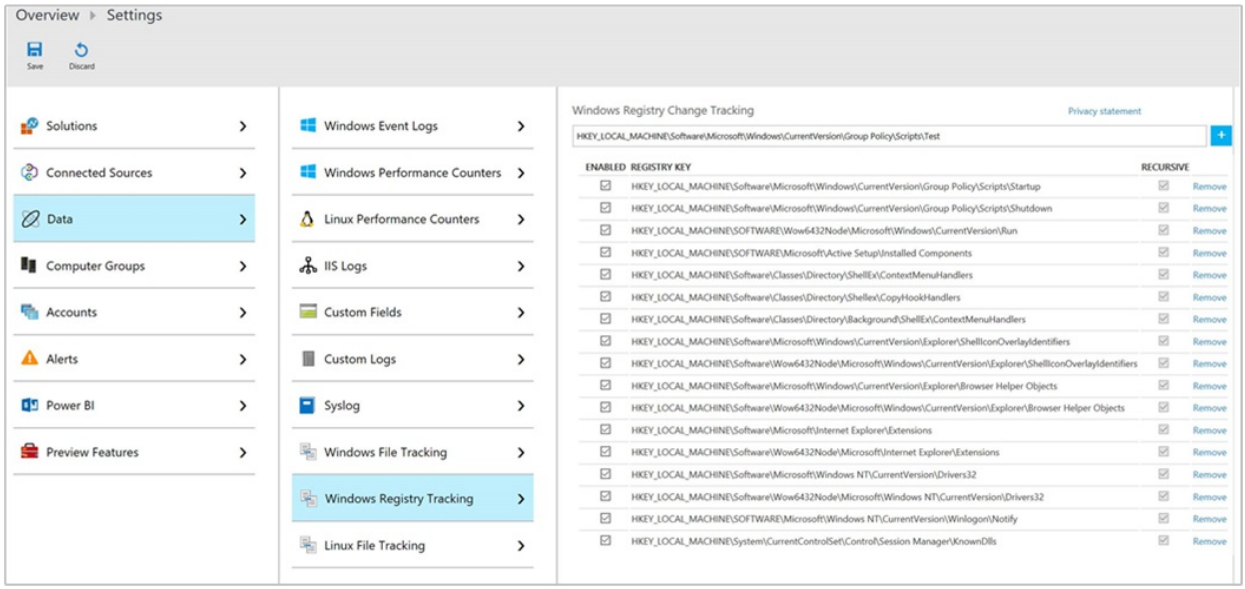
1. In the OMS portal, click **Settings** (the gear symbol).
2. On the **Settings** page, click **Data**, and then click **Windows File Tracking**.
3. Under Windows File Change Tracking, type the entire path, including the file name of the file that you want to track and then click the **Add** symbol. For example: C:\Program Files (x86)\Internet Explorer\iexplore.exe or C:\Windows\System32\drivers\etc\hosts.
4. Click **Save**.



Configure Windows registry keys to track

Use the following steps to configure registry keys to track on Windows computers.

1. In the OMS portal, click **Settings** (the gear symbol).
2. On the **Settings** page, click **Data**, and then click **Windows Registry Tracking**.
3. Under Windows Registry Change Tracking, type the entire key that you want to track and then click the **Add** symbol.
4. Click **Save**.



Limitations

The Change Tracking solution does not currently support the following:

- folders (directories)
- recursion
- wild cards
- path variables
- network file systems

Other limitations:

- The **Max File Size** column and values are unused in the current implementation.
- If you collect more than 2500 files in the 30-minute collection cycle, solution performance might be degraded.
- When network traffic is high, change records may take up to a maximum of six hours to display.
- If you modify the configuration while a computer is shut down, the computer might post file changes that belonged to the previous configuration.

Change Tracking data collection details

Change Tracking collects software inventory and Windows Service metadata using the agents that you have enabled.

The following table shows data collection methods and other details about how data is collected for Change Tracking.

PLATFORM	DIRECT AGENT	SCOM AGENT	LINUX AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY

PLATFORM	DIRECT AGENT	SCOM AGENT	LINUX AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows and Linux							5 minutes to 50 minutes, depending on the change type. See below for more information.

The following table shows the data collection frequency for the types of changes.

CHANGE TYPE	FREQUENCY	DOES AGENT SEND DIFFERENCES WHEN FOUND?
Windows registry	50 minutes	No
Windows file	30 minutes	Yes. If there is no change in 24 hours, a snapshot is sent.
Linux file	15 minutes	Yes. If there is no change in 24 hours, a snapshot is sent.
Windows services	30 minutes	Yes, every 30 minutes when changes are found. Every 24 hours a snapshot is sent, regardless of change. So, the snapshot is sent even where there are no changes.
Linux daemons	5 minutes	Yes. If there is no change in 24 hours, a snapshot is sent.
Windows software	30 minutes	Yes, every 30 minutes when changes are found. Every 24 hours a snapshot is sent, regardless of change. So, the snapshot is sent even where there are no changes.
Linux software	5 minutes	Yes. If there is no change in 24 hours, a snapshot is sent.

Registry key change tracking

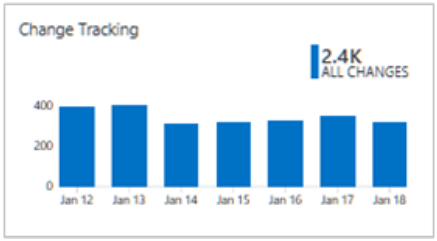
Log Analytics performs Windows registry monitoring and tracking with the Change Tracking solution. The purpose of monitoring changes to registry keys is to pinpoint extensibility points where third-party code and malware can activate. The following list shows the default registry keys that are tracked by the solution and why each is tracked.

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup
  - Monitors scripts that run at startup.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown
  - Monitors scripts that run at shutdown.
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
  - Monitors keys that are loaded before the user signs in their Windows account for 32-bit programs running on 64-bit computers.
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components
  - Monitors changes to application settings.

- HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\ContextMenuHandlers
  - Monitors common autostart entries that hook directly into Windows Explorer and usually run in-process with Explorer.exe.
- HKEY_LOCAL_MACHINE\Software\Classes\Directory\Shellex\CopyHookHandlers
  - Monitors common autostart entries that hook directly into Windows Explorer and usually run in-process with Explorer.exe.
- HKEY_LOCAL_MACHINE\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers
  - Monitors common autostart entries that hook directly into Windows Explorer and usually run in-process with Explorer.exe.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
  - Monitors for icon overlay handler registration.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
  - Monitors for icon overlay handler registration for 32-bit programs running on 64-bit computers.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
  - Monitors for new browser helper object plugins for Internet Explorer, which can be used to access the Document Object Model (DOM) of the current page and to control navigation.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
  - Monitors for new browser helper object plugins for Internet Explorer, which can be used to access the Document Object Model (DOM) of the current page and to control navigation for 32-bit programs running on 64-bit computers.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Extensions
  - Monitors for new Internet Explorer extensions, such as custom tool menus and custom toolbar buttons.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions
  - Monitors for new Internet Explorer extensions, such as custom tool menus and custom toolbar buttons for 32-bit programs running on 64-bit computers.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
  - Monitors the 32-bit drivers associated with wavemapper, wave1 and wave2, msacm.imaadpcm, .msadpcm, .msgsm610, and vidc. Similar to the [drivers] section in the SYSTEM.INI file.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
  - Monitors the 32-bit drivers associated with wavemapper, wave1 and wave2, msacm.imaadpcm, .msadpcm, .msgsm610, and vidc for 32-bit programs running on 64-bit computers. Similar to the [drivers] section in the SYSTEM.INI file.
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDlls
  - Monitors the list of known or commonly used system DLLs; this system prevents people from exploiting weak application directory permissions by dropping in Trojan horse versions of system DLLs.
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
  - Monitors the list of packages able to receive event notifications from Winlogon, the interactive logon support model for the Windows operating system.

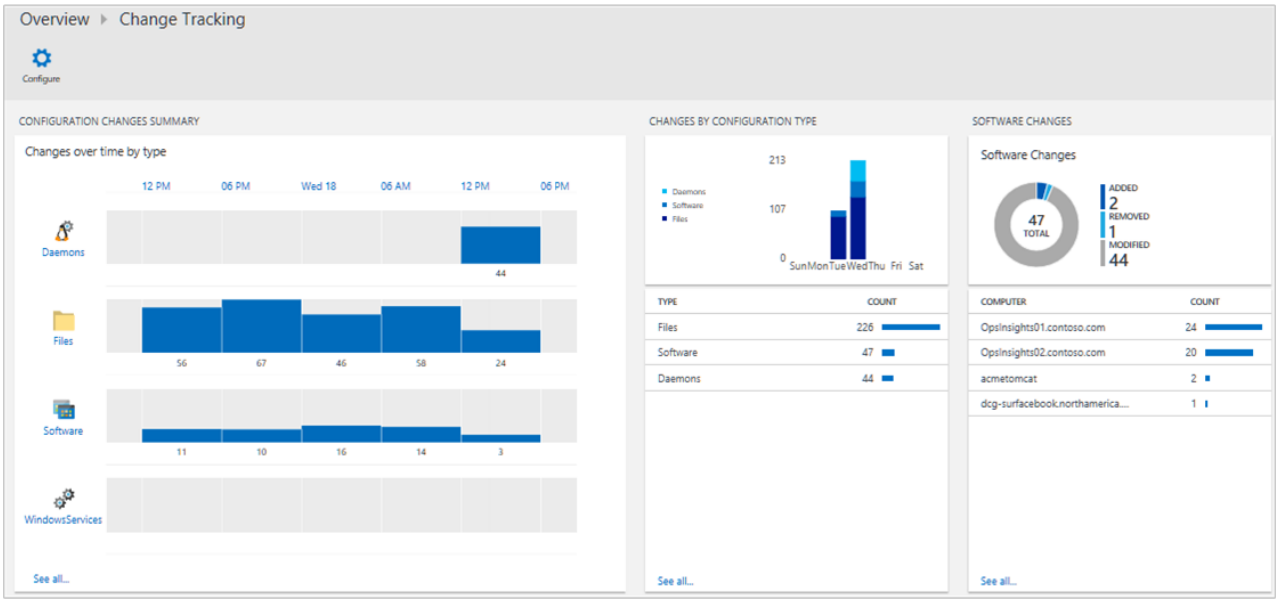
Use Change Tracking

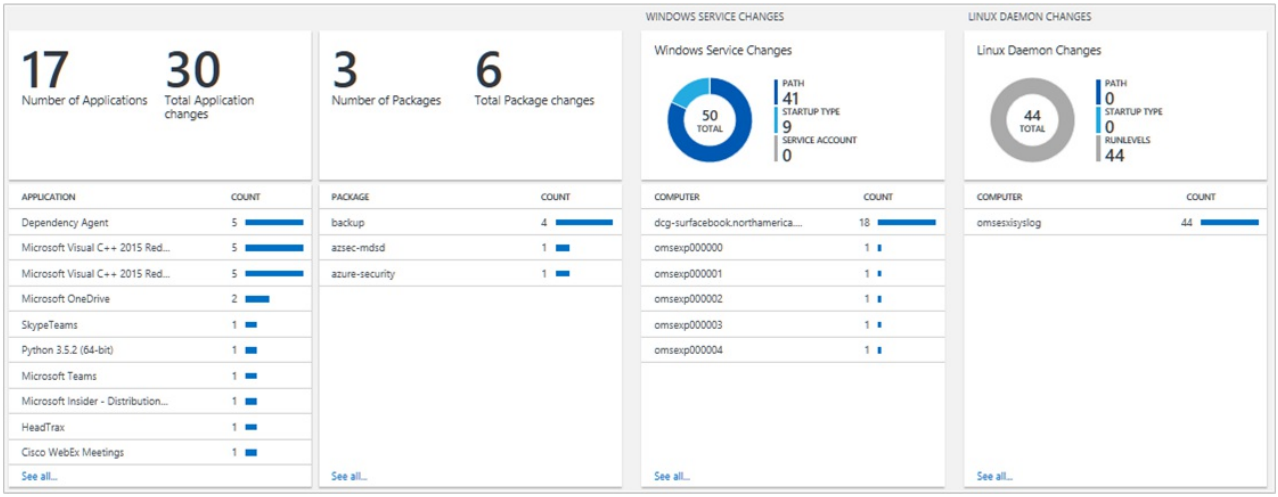
After the solution is installed, you can view the summary of changes for your monitored servers by using the **Change Tracking** tile on the **Overview** page in OMS.



You can view changes to your infrastructure and then drill-into details for the following categories:

- Changes by configuration type for software and Windows services
- Software changes to applications and updates for individual servers
- Total number of software changes for each application
- Linux packages
- Windows service changes for individual servers
- Linux daemon changes





To view changes for any change type

1. On the **Overview** page, click the **Change Tracking** tile.
2. On the **Change Tracking** dashboard, review the summary information in one of the change type blades and then click one to view detailed information about it in the **log search** page.
3. On any of the log search pages, you can view results by time, detailed results, and your log search history. You can also filter by facets to narrow the results.

Next steps

- Use Log searches in Log Analytics to view detailed change tracking data.

Update Management solution in OMS

5/3/2017 • 18 min to read • Edit Online

The Update Management solution in OMS allows you to manage updates for your Windows and Linux computers. You can quickly assess the status of available updates on all agent computers and initiate the process of installing required updates for servers.

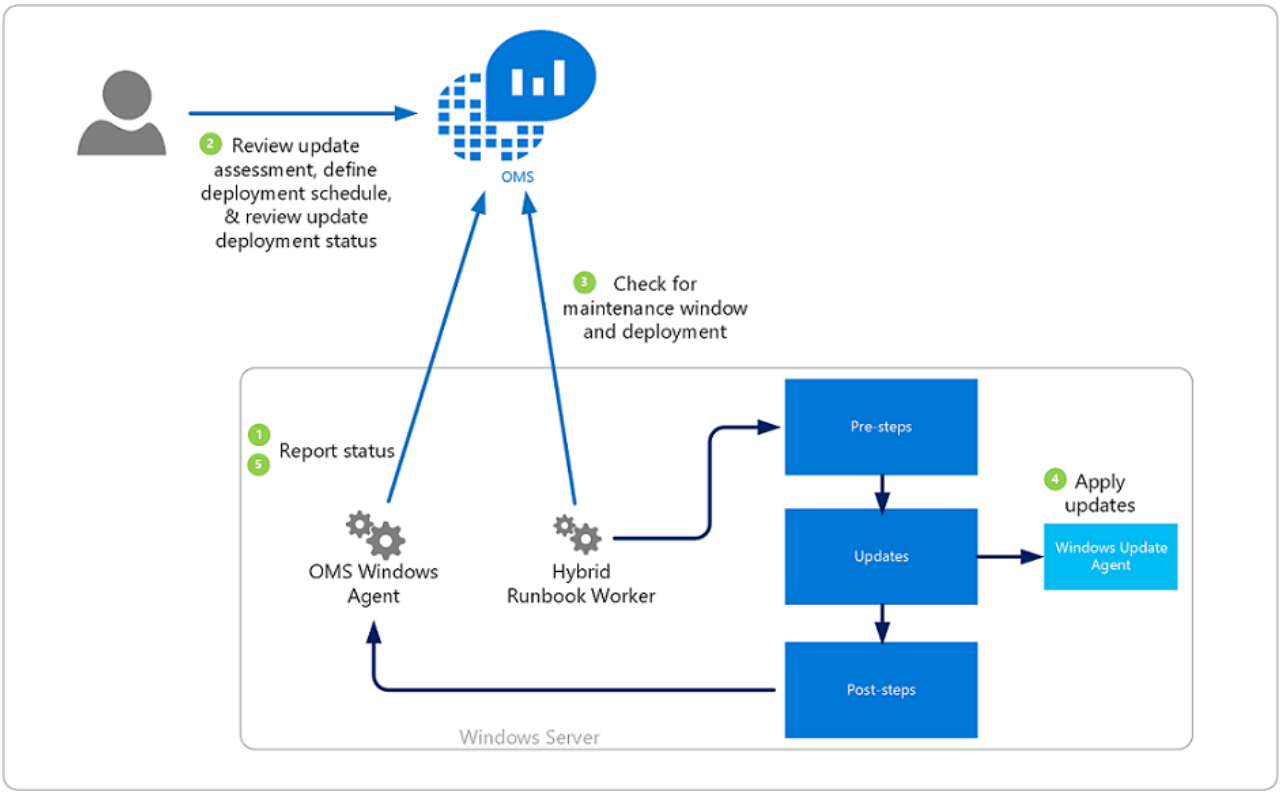
Solution components

Computers managed by OMS use the following for performing assessment and update deployments:

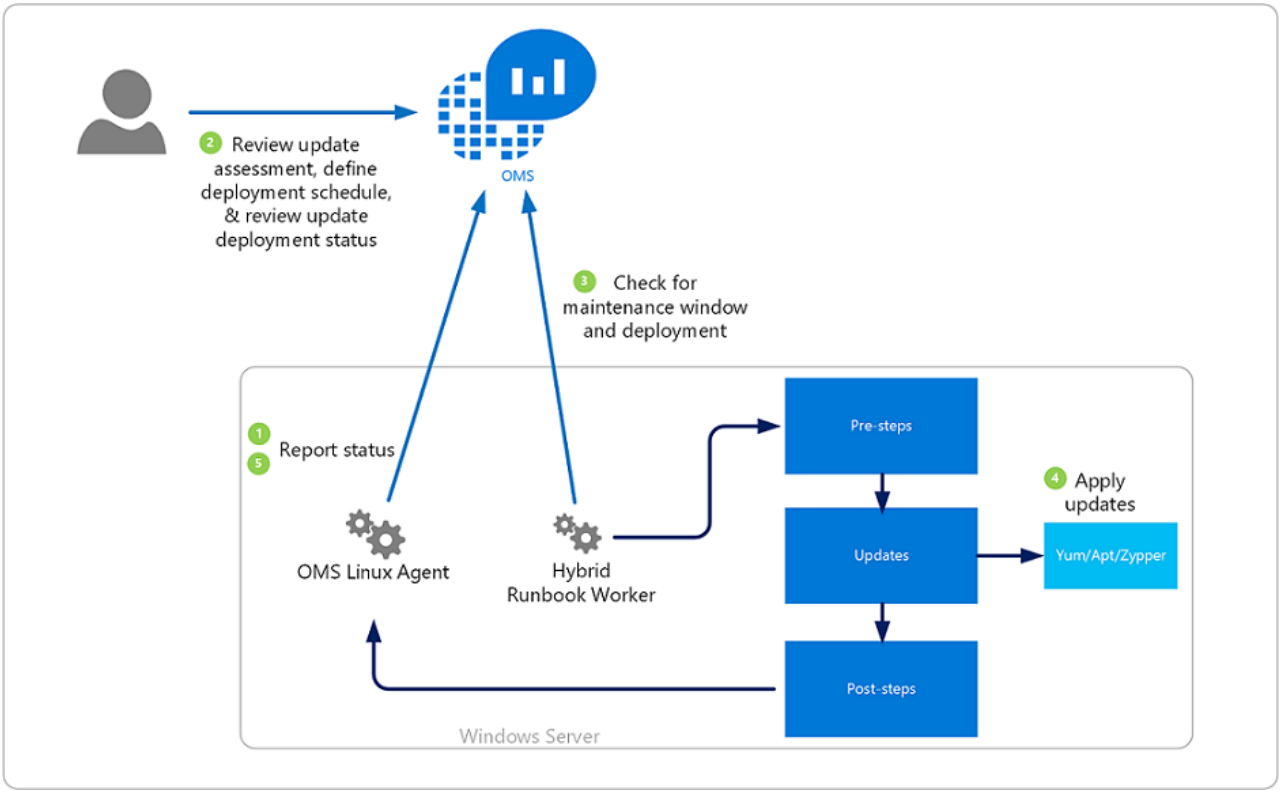
- OMS agent for Windows or Linux
- PowerShell Desired State Configuration (DSC) for Linux
- Automation Hybrid Runbook Worker
- Microsoft Update or Windows Server Update Services for Windows computers

The following diagrams shows a conceptual view of the behavior and data flow with how the solution assesses and applies updates to all connected Windows Server and Linux computers in a workspace.

Windows Server



Linux



After the computer performs a scan for update compliance, the OMS agent forwards the information in bulk to OMS. On a Window computer, the compliance scan is performed every 12 hours by default. In addition to the scan schedule, the scan for update compliance is initiated within 15 minutes if the Microsoft Monitoring Agent (MMA) is restarted, prior to update installation, and after update installation. With a Linux computer, the compliance scan is performed every 3 hours by default, and a compliance scan is initiated within 15 minutes if the MMA agent is restarted.

The compliance information is then processed and summarized in the dashboards included in the solution or searchable using user-defined or pre-defiend queries. The solution reports how up-to-date the computer is based on what source you are configured to synchronize with. If the Windows computer is configured to report to WSUS, depending on when WSUS last synchronized with Microsoft Update, the results may differ from what Microsoft Updates shows. The same for Linux computers that are configured to report to a local repo versus a public repo.

You can deploy and install software updates on computers that require the updates by creating a scheduled deployment. Updates classified as *Optional* are not included in the deployment scope for Windows computers, only required updates. The scheduled deployment defines what target computers will receive the applicable updates, either by explicitly specifying computers or selecting a computer group that is based off of log searches of a particular set of computers. You also specify a schedule to approve and designate a period of time when updates are allowed to be installed within. Updates are installed by runbooks in Azure Automation. You cannot view these runbooks, and they don't require any configuration. When an Update Deployment is created, it creates a schedule that starts a master update runbook at the specified time for the included computers. This master runbook starts a child runbook on each agent that performs installation of required updates.

At the date and time specified in the update deployment, the target computers executes the deployment in parallel. A scan is first performed to verify the updates are still required and installs them. It is important to note for WSUS client computers, if the updates are not approved in WSUS, the update deployment will fail. The results of the applied updates are forwarded to OMS to be processed and summarized in the dashboards or by the searching the events.

Prerequisites

- The solution supports performing update assessments against Windows Server 2008 and higher, and update deployments against Windows Server 2012 and higher. Server Core and Nano Server installation options are

not supported.

- Windows client operating systems are not supported.
- Windows agents must either be configured to communicate with a Windows Server Update Services (WSUS) server or have access to Microsoft Update.

> **NOTE**
> The Windows agent cannot be managed concurrently by System Center Configuration Manager.

- CentOS 6 (x86/x64), and 7 (x64)
- Red Hat Enterprise 6 (x86/x64), and 7 (x64)
- SUSE Linux Enterprise Server 11 (x86/x64) and 12 (x64)
- Ubuntu 12.04 LTS and newer x86/x64
- Linux agents must have access to an update repository.

> **NOTE**
> An OMS Agent for Linux configured to report to multiple OMS workspaces is not supported with this solution.

For additional information on how to install the OMS Agent for Linux and download the latest version, refer to Operations Management Suite Agent for Linux. For information on how to install the OMS Agent for Windows, review Operations Management Suite Agent for Windows.

Solution components

This solution consists of the following resources that are added to your Automation account and directly connected agents or Operations Manager connected management group.

Management packs

If your System Center Operations Manager management group is connected to an OMS workspace, the following management packs are installed in Operations Manager. These management packs are also installed on directly connected Windows computers after adding this solution. There is nothing to configure or manage with these management packs.

- Microsoft System Center Advisor Update Assessment Intelligence Pack (Microsoft.IntelligencePacks.UpdateAssessment)
- Microsoft.IntelligencePack.UpdateAssessment.Configuration (Microsoft.IntelligencePack.UpdateAssessment.Configuration)
- Update Deployment MP

For more information on how solution management packs are updated, see Connect Operations Manager to Log Analytics.

Hybrid Worker groups

After you enable this solution, any Windows computer directly connected to your OMS workspace is automatically configured as a Hybrid Runbook Worker to support the runbooks included in this solution. For each Windows computer managed by the solution, it will be listed under the Hybrid Runbook Worker Groups blade of the Automation account following the naming convention *Hostname FQDN_GUID*. You cannot target these groups with runbooks in your account, otherwise they will fail. These groups are only intended to support the management solution.

You can however, add the Windows computers to a Hybrid Runbook Worker group in your Automation account to support Automation runbooks as long as you are using the same account for both the solution and Hybrid

Runbook Worker group membership. This functionality has been added to version 7.2.12024.0 of the Hybrid Runbook Worker.

Configuration

Perform the following steps to add the Update Management solution to your OMS workspace and confirm agents are reporting. Windows agents already connected to your workspace are added automatically with no additional configuration.

You can deploy the solution using the following methods:

- From Azure Marketplace in the Azure portal by selecting either the Automation & Control offering or Update Management solution
- From the OMS Solutions Gallery in your OMS workspace

If you already have an Automation account and OMS workspace linked together in the same resource group and region, selecting Automation & Control will verify your configuration and only install the solution and configure it in both services. Selecting the Update Management solution from Azure Marketplace delivers the same behavior. If you do not have either services deployed in your subscription, follow the steps in the **Create new Solution** blade and confirm you want to install the other pre-selected recommended solutions. Optionally, you can add the Update Management solution to your OMS workspace using the steps described in Add OMS solutions from the Solutions Gallery.

Confirm OMS agents and Operations Manager management group connected to OMS

To confirm directly connected OMS Agent for Linux and Windows are communicating with OMS, after a few minutes you can run the following log search:

- Linux - `Type=Heartbeat OSType=Linux | top 500000 | dedup SourceComputerId | Sort Computer | display Table`.
- Windows -
  `Type=Heartbeat OSType=Windows | top 500000 | dedup SourceComputerId | Sort Computer | display Table`

On a Windows computer, you can review the following to verify agent connectivity with OMS:

1. Open Microsoft Monitoring Agent in Control Panel, and on the **Azure Log Analytics (OMS)** tab, the agent displays a message stating: **The Microsoft Monitoring Agent has successfully connected to the Microsoft Operations Management Suite service**.
2. Open the Windows Event Log, navigate to **Application and Services Logs\Operations Manager** and search for Event ID 3000 and 5002 from source Service Connector. These events indicate the computer has registered with the OMS workspace and is receiving configuration.

If the agent is not able to communicate with the OMS service and it is configured to communicate with the internet through a firewall or proxy server, confirm the firewall or proxy server is properly configured by reviewing Configure proxy and firewall settings in Log Analytics.

Newly added Linux agents will show a status of **Updated** after an assessment has been performed. This process can take up to 6 hours.

To confirm an Operations Manager management group is communicating with OMS, see Validate Operations Manager Integration with OMS.

Data collection

Supported agents

The following table describes the connected sources that are supported by this solution.

CONNECTED SOURCE	SUPPORTED	DESCRIPTION
Windows agents	Yes	The solution collects information about system updates from Windows agents and initiates installation of required updates.
Linux agents	Yes	The solution collects information about system updates from Linux agents and initiates installation of required updates on supported distros.
Operations Manager management group	Yes	The solution collects information about system updates from agents in a connected management group. A direct connection from the Operations Manager agent to Log Analytics is not required. Data is forwarded from the management group to the OMS repository.
Azure storage account	No	Azure storage does not include information about system updates.

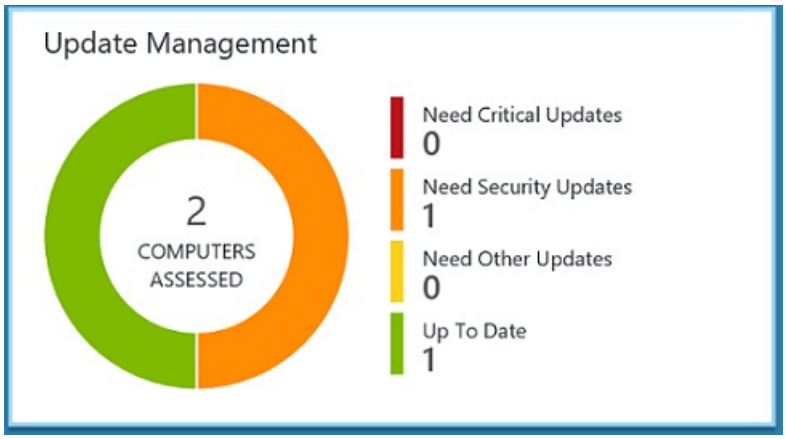
Collection frequency

For each managed Windows computer, a scan is performed twice per day. Every 15 minutes the Windows API is called to query for the last update time to determine if status has changed, and if so a compliance scan is initiated. For each managed Linux computer, a scan is performed every 3 hours.

It can take anywhere from 30 minutes up to 6 hours for the dashboard to display updated data from managed computers.

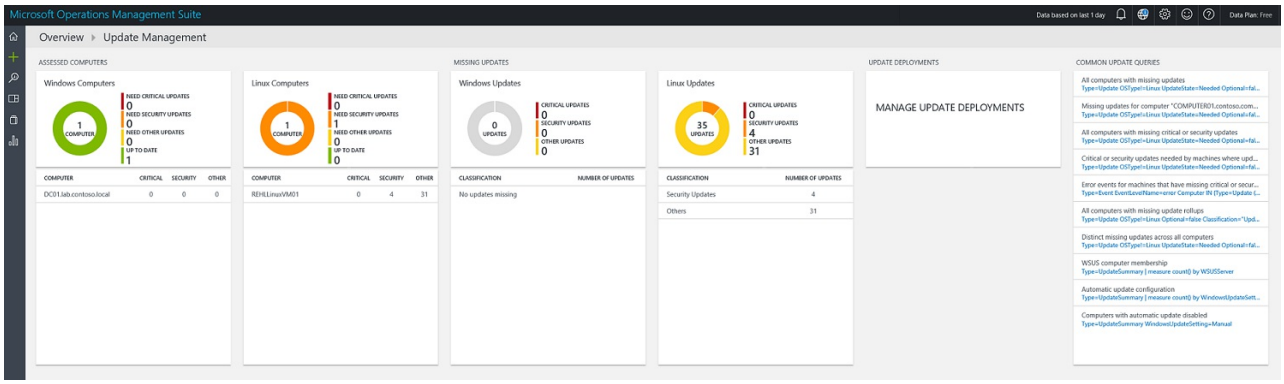
Using the solution

When you add the Update Management solution to your OMS workspace, the **Update Management** tile will be added to your OMS dashboard. This tile displays a count and graphical representation of the number of computers in your environment and their update compliance.



Viewing update assessments

Click on the **Update Management** tile to open the **Update Management** dashboard.



This dashboard provides a detailed breakdown of update status categorized by type of operating system and update classification - critical, security, or other (such as a definition update). The **Update Deployments** tile when selected, redirects you to the Update Deployments page where you can view schedules, deployments currently running, completed deployments, or schedule a new deployment.

You can run a log search that returns all records by clicking on the specific tile or to run a query of a particular category and pre-defined criteria , select one from the list available under the **Common Update Queries** column.

Installing updates

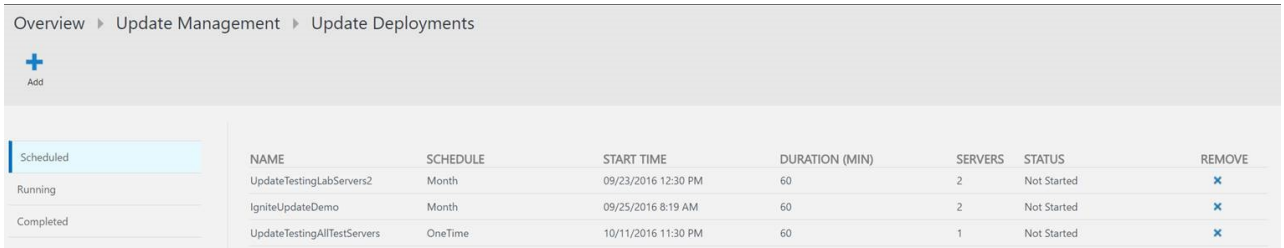
Once updates have been assessed for all of the Linux and Windows computers in your workspace, you can have required updates installed by creating an *Update Deployment*. An Update Deployment is a scheduled installation of required updates for one or more computers. You specify the date and time for the deployment in addition to a computer or group of computers that should be included in the scope of a deployment. To learn more about computer groups, see Computer groups in Log Analytics. When you include computer groups in your update deployment, group memnbership is evaluated only once at the time of schedule creation. Subsequent changes to a group are not reflected. To work around this, delete the scheduled update deployment and recreate it.

> **NOTE**
>
> Windows VMs deployed from the Azure Marketplace by default are set to receive automatic updates from Windows Update Service. This behavior does not change after adding this solution or Windows VMs to your workspace. If you do not actively managed updates with this solution, the default behavior (automatically apply updates) will apply.

For virtual machines created from the on-demand Red Hat Enterprise Linux (RHEL) images available in Azure Marketplace, they are registered to access the Red Hat Update Infrastructure (RHUI) deployed in Azure. Any other Linux distribution must be updated from the distros online file repository following their supported methods.

Viewing update deployments

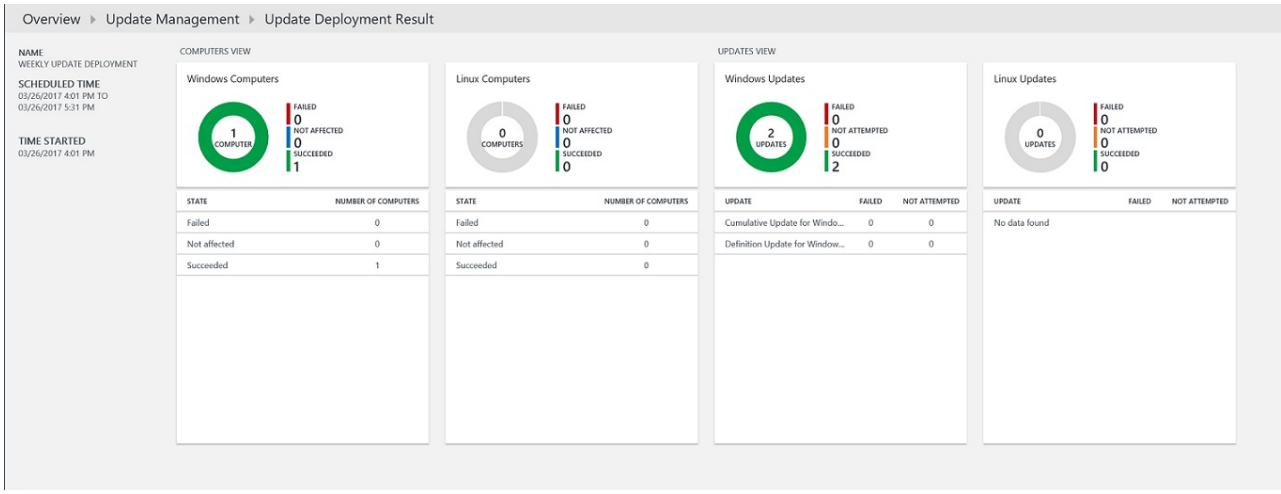
Click the **Update Deployment** tile to view the list of existing Update Deployments. They are grouped by status – **Scheduled**, **Running**, and **Completed**.



The properties displayed for each Update Deployment are described in the following table.

PROPERTY	DESCRIPTION
Name	Name of the Update Deployment.
Schedule	Type of schedule. Options available are *One Time*, *Recurring Weekly*, or *Recurring Monthly*.
Start Time	Date and time that the Update Deployment is scheduled to start.
Duration	Number of minutes the Update Deployment is allowed to run. If all updates are not installed within this duration, then the remaining updates must wait until the next Update Deployment.
Servers	Number of computers affected by the Update Deployment.
Status	Current status of the Update Deployment. Possible values are: - Not Started - Running - Finished

Select a completed Update Deployment to view the detail screen which includes the columns in the following table. These columns will not be populated if the Update Deployment has not yet started.



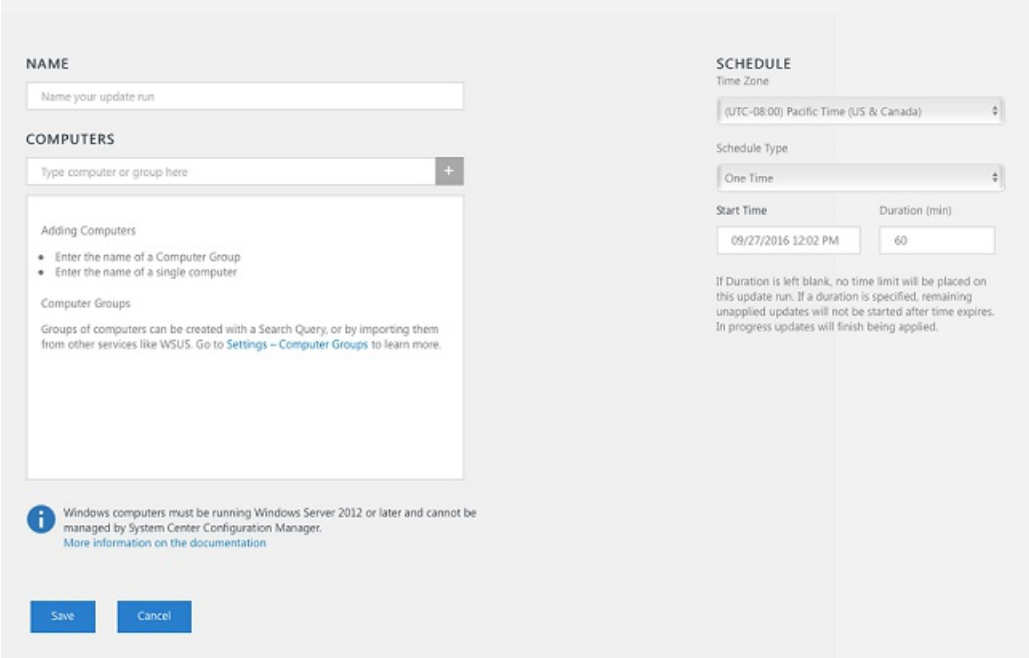
COLUMN	DESCRIPTION
Computers View	
Windows Computers	Lists the number of Windows computers in the Update Deployment by status. Click on a status to run a log search returning all update records with that status for the Update Deployment.
Linux Computers	Lists the number of Linux computers in the Update Deployment by status. Click on a status to run a log search returning all update records with that status for the Update Deployment.

COLUMN	DESCRIPTION
Computer Installation Status	Lists the computers involved in the Update Deployment and the percentage of updates that successfully installed. Click on one of the entries to run a log search returning all missing and critical updates.
Updates View	
Windows Updates	Lists Windows updates included in the Update Deployment and their installation status per each update. Select an update to run a log search returning all update records for that specific update or click on the status to run a log search returning all update records for the deployment.
Linux Updates	Lists Linux updates included in the Update Deployment and their installation status per each update. Select an update to run a log search returning all update records for that specific update or click on the status to run a log search returning all update records for the deployment.

Creating an Update Deployment

Create a new Update Deployment by clicking the **Add** button at the top of the screen to open the **New Update Deployment** page. You must provide values for the properties in the following table.

PROPERTY	DESCRIPTION
Name	Unique name to identify the update deployment.
Time Zone	Time zone to use for the start time.
Schedule Type	Type of schedule. Options available are *One Time*, *Recurring Weekly*, or *Recurring Monthly*.
Start Time	Date and time to start the update deployment. **Note:** The soonest a deployment can run is 30 minutes from current time if you need to deploy immediately.
Duration	Number of minutes the Update Deployment is allowed to run. If all updates are not installed within this duration, then the remaining updates must wait until the next Update Deployment.
Computers	Names of computers or computer groups to include and target in the Update Deployment. Select one or more entries from the drop down list.



Time range

By default, the scope of the data analyzed in the Update Management solution is from all connected management groups generated within the last 1 day.

To change the time range of the data, select **Data based on** at the top of the dashboard. You can select records created or updated within the last 7 days, 1 day, or 6 hours. Or you can select **Custom** and specify a custom date range.

Log Analytics records

The Update Management solution creates two types of records in the OMS repository.

Update records

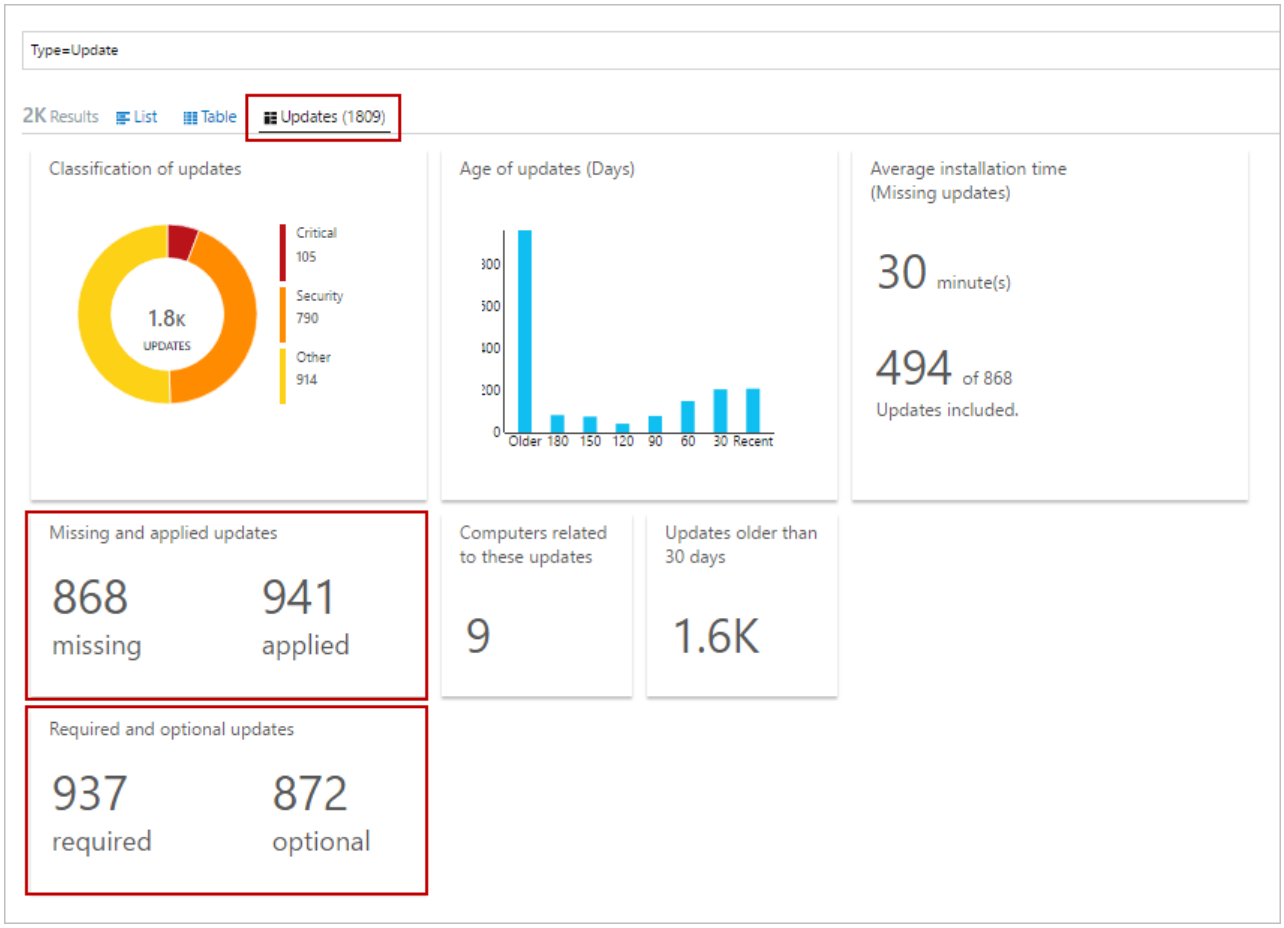
A record with a type of **Update** is created for each update that is either installed or needed on each computer. Update records have the properties in the following table.

PROPERTY	DESCRIPTION
Type	*Update*
SourceSystem	The source that approved installation of the update. Possible values are: - Microsoft Update - Windows Update - SCCM - Linux Servers (Fetched from Package Managers)
Approved	Specifies whether the update has been approved for installation. For Linux servers this is currently optional as patching is not managed by OMS.

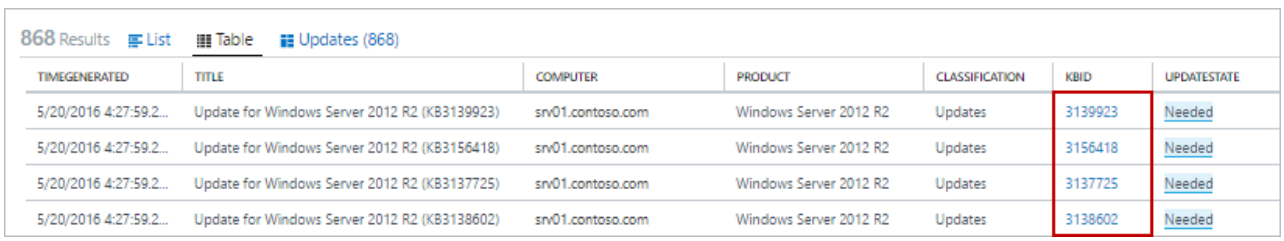
PROPERTY	DESCRIPTION
Classification for Windows	Classification of the update. Possible values are: - Applications - Critical Updates - Definition Updates - Feature Packs - Security Updates - Service Packs - Update Rollups - Updates
Classification for Linux	Cassification of the update. Possible values are: -Critical Updates - Security Updates - Other Updates
Computer	Name of the computer.
InstallTimeAvailable	Specifies whether the installation time is available from other agents that installed the same update.
InstallTimePredictionSeconds	Estimated installation time in seconds based on other agents that installed the same update.
KBID	ID of the KB article that describes the update.
ManagementGroupName	Name of the management group for SCOM agents. For other agents, this is AOI-.
MSRCBulletinID	ID of the Microsoft security bulletin describing the update.
MSRCSeverity	Severity of the Microsoft security bulletin. Possible values are: - Critical - Important - Moderate
Optional	Specifies whether the update is optional.
Product	Name of the product the update is for. Click **View** to open the article in a browser.
PackageSeverity	The severity of the vulnerability fixed in this update, as reported by the Linux distro vendors.
PublishDate	Date and time that the update was installed.
RebootBehavior	Specifies if the update forces a reboot. Possible values are: - canrequestreboot - neverreboots
RevisionNumber	Revision number of the update.

PROPERTY	DESCRIPTION
SourceComputerId	GUID to uniquely identify the computer.
TimeGenerated	Date and time that the record was last updated.
Title	Title of the update.
UpdateID	GUID to uniquely identify the update.
UpdateState	Specifies whether the update is installed on this computer. Possible values are: - Installed - The update is installed on this computer. - Needed - The update is not installed and is needed on this computer.

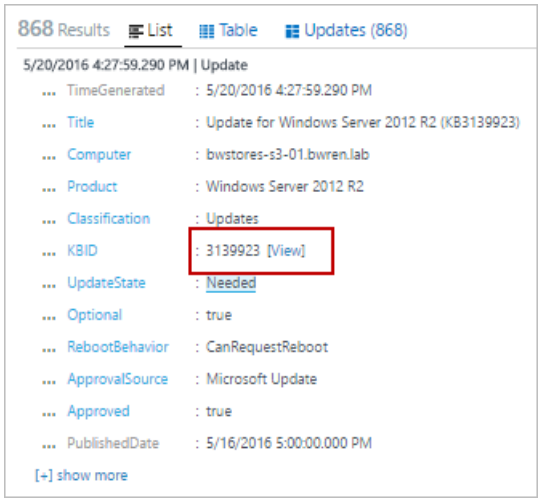
When you perform any log search that returns records with a type of **Update** you can select the **Updates** view which displays a set of tiles summarizing the updates returned by the search. You can click on the entries in the **Missing and applied updates** and **Required and optional updates** tiles to scope the view to that set of updates. Select the **List** or **Table** view to return the individual records.



In the **Table** view, you can click on the **KBID** for any record to open a browser with the KB article. This allows you to quickly read about the details of the particular update.



In the **List** view, you click the **View** link next to the KBID to open the KB article.



UpdateSummary records

A record with a type of **UpdateSummary** is created for each Windows agent computer. This record is updated each time the computer is scanned for updates. **UpdateSummary** records have the properties in the following table.

PROPERTY	DESCRIPTION
Type	UpdateSummary
SourceSystem	OpsManager
Computer	Name of the computer.
CriticalUpdatesMissing	Number of critical updates missing on the computer.
ManagementGroupName	Name of the management group for SCOM agents. For other agents, this is AOI-.
NETRuntimeVersion	Version of the .NET runtime installed on the computer.
OldestMissingSecurityUpdateBucket	Bucket to categorize the time since the oldest missing security update on this computer was published. Possible values are: - Older - 180 days ago - 150 days ago - 120 days ago - 90 days ago - 60 days ago - 30 days go - Recent
OldestMissingSecurityUpdateInDays	Number of days since the oldest missing security update on this computer was published.
OsVersion	Version of the operating system installed on the computer.
OtherUpdatesMissing	Number of other updates missing on the computer.

PROPERTY	DESCRIPTION
SecurityUpdatesMissing	Number of security updates missing on the computer.
SourceComputerId	GUID to uniquely identify the computer.
TimeGenerated	Date and time that the record was last updated.
TotalUpdatesMissing	Total number of updates missing on the computer.
WindowsUpdateAgentVersion	Version number of the Windows Update agent on the computer.
WindowsUpdateSetting	Setting for how the computer will install important updates. Possible values are: - Disabled - Notify before installation - Scheduled installation
WSUSServer	URL of WSUS server if the computer is configured to use one.

Sample log searches

The following table provides sample log searches for update records collected by this solution.

QUERY	DESCRIPTION
Windows-based server computers that need updates	`Type:Update OSType!=Linux UpdateState=Needed Optional=false Approved!=false
Linux servers that need updates	`Type:Update OSType=Linux UpdateState!="Not needed"
All computers with missing updates	`Type=Update UpdateState=Needed Optional=false
Missing updates for a specific computer (replace value with your own computer name)	`Type=Update UpdateState=Needed Optional=false Computer="COMPUTER01.contoso.com"
All computers with missing critical or security updates	`Type=Update UpdateState=Needed Optional=false (Classification="Security Updates" OR Classification="Critical Updates")
Critical or security updates needed by machines where updates are manually applied	`Type=Update UpdateState=Needed Optional=false (Classification="Security Updates" OR Classification="Critical Updates") Computer IN {Type=UpdateSummary WindowsUpdateSetting=Manual
Error events for machines that have missing critical or security required updates	`Type=Event EventLevelName=error Computer IN {Type=Update (Classification="Security Updates" OR Classification="Critical Updates") UpdateState=Needed Optional=false
All computers with missing update rollups	`Type=Update Optional=false Classification="Update Rollups" UpdateState=Needed

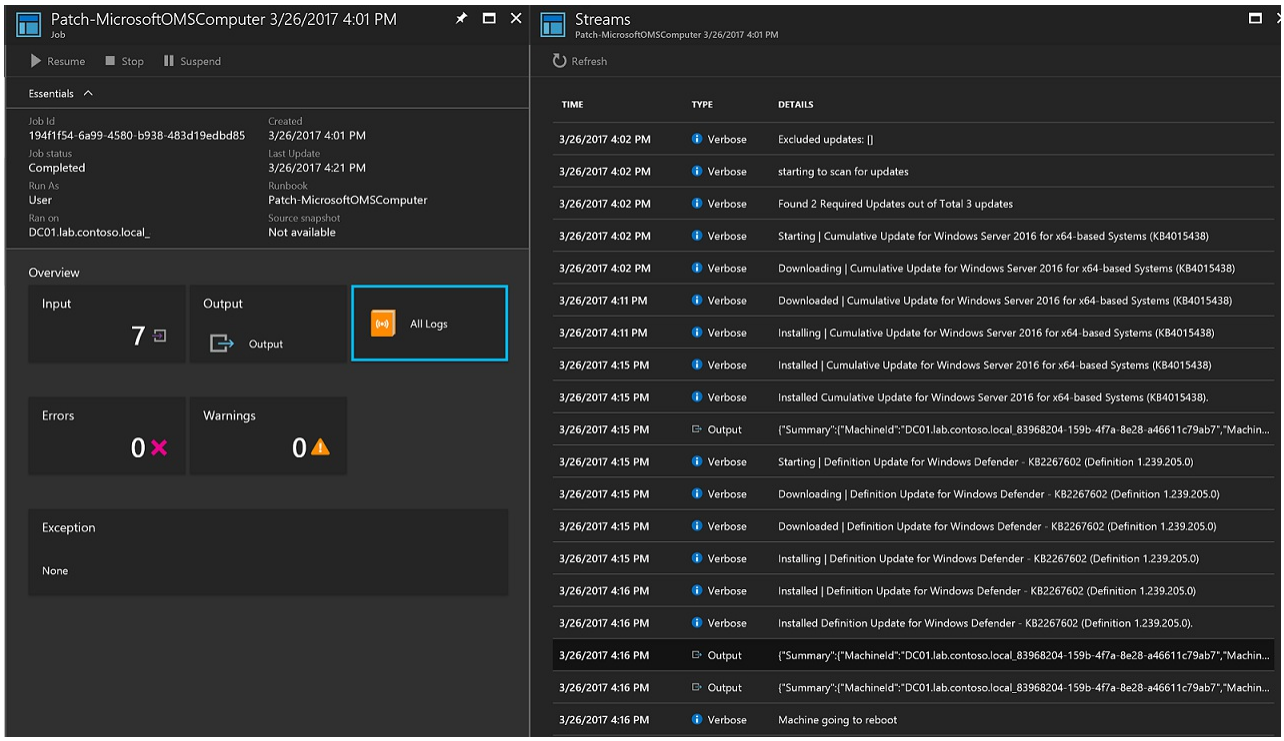
QUERY	DESCRIPTION
Distinct missing updates across all computers	`Type=Update UpdateState=Needed Optional=false
Windows-based server computer with updates that failed in an update run	`Type:UpdateRunProgress InstallationStatus=failed
Linux server with updates that failed an update run	`Type:UpdateRunProgress InstallationStatus=failed
WSUS computer membership	`Type=UpdateSummary
Automatic update configuration	`Type=UpdateSummary
Computers with automatic update disabled	`Type=UpdateSummary WindowsUpdateSetting=Manual`
List of all the Linux machines which have a package update available	`Type=Update and OSType=Linux and UpdateState!="Not needed"
List of all the Linux machines which have a package update available which addresses Critical or Security vulnerability	`Type=Update and OSType=Linux and UpdateState!="Not needed" and (Classification="Critical Updates" OR Classification="Security Updates")
List of all packages that have an update available	Type=Update and OSType=Linux and UpdateState!="Not needed"
List of all packages that have an update available which addresses Critical or Security vulnerability	`Type=Update and OSType=Linux and UpdateState!="Not needed" and (Classification="Critical Updates" OR Classification="Security Updates")`
List what update deployments have modified computers	`Type:UpdateRunProgress
Computers that were updated in this update run (replace value with your Update Deployment name	`Type:UpdateRunProgress UpdateRunName="DeploymentName"
List of all the “Ubuntu” machines with any update available	`Type=Update and OSType=Linux and OSName = Ubuntu &

Troubleshooting

This section provides information to help troubleshoot issues with the Update Management solution.

How do I troubleshoot update deployments?

You can view the results of the runbook responsible for deploying the updates included in the scheduled update deployment from the Jobs blade of your Automation account that is linked with the OMS workspace supporting this solution. The runbook **Patch-MicrosoftOMSComputer** is a child runbook that targets a specific managed computer, and reviewing the verbose Stream will present detailed information for that deployment. The output will display which required updates are applicable, download status, installation status, and additional details.



For further information, see Automation runbook output and messages.

Next steps

- Use Log Searches in Log Analytics to view detailed update data.
- Create your own dashboards showing update compliance for your managed computers.
- Create alerts when critical updates are detected as missing from computers or a computer has automatic updates disabled.

Identify malware using the Malware Assessment solution in Log Analytics

3/27/2017 • 3 min to read • Edit Online

You can use the Antimalware solution in Log Analytics to report on the status of antimalware protection in your infrastructure. Installing the solution updates the OMS agent and base configuration for OMS. Antimalware protection status and detected threats on the monitored servers are read, and then the data is sent to the Log Analytics service in the cloud for processing. Logic is applied to the received data and the cloud service records the data. Servers with detected threats and servers with insufficient protection are shown in the **Antimalware** dashboard. By using the information on the **Antimalware** dashboard, you can identify a plan to apply protection to the servers that need it.

Installing and configuring the solution

Use the following information to install and configure the solution.

- In order to use the Malware Assessment solution, you must subscribe to the Security & Compliance solution offering.
- Add the Malware Assessment solution to your OMS workspace from Azure marketplace or by using the process described in Add Log Analytics solutions from the Solutions Gallery. There is no further configuration required.

Use Antimalware

Log Analytics reports antimalware status for:

- Computers running Windows Defender on Windows 8, Windows 8.1, Windows 10, and Windows Server 2016 TP4 or later
- Windows Security Center (WSC) on Windows 8, Windows 8.1, Windows 10, Windows Server 2016 TP4 or later
- Servers running System Center Endpoint Protection (v4.5.216 or later), Azure virtual machines with the antimalware extension, and Windows Malicious Software Removal Tool (MSRT)
- Servers with Windows Management Framework 3 (or later) WMF 3.0, WMF 4.0.
- Symantec Endpoint Protection 12.x and 14.x versions
- Trend Micro Deep Security version 9.6

In addition to detecting when 3rd party solutions are installed, an additional assessment is also done to determine whether protection by agents is operational. Specifically, OMS Security tests to see if the antimalware agents from these vendors on the monitored servers are:

- Enabled
- Running scans at regular intervals
- Using signatures no older than seven days

The antimalware solution does not currently report on:

- Servers running Windows Server 2008 and earlier
- Web and Worker roles in Microsoft Azure

You can help us prioritize the addition of new features by voting or adding a new suggestion on our feedback page.

Malware Assessment data collection details

Malware Assessment collects configuration data, metadata, and state data using the agents that you have enabled.

The following table shows data collection methods and other details about how data is collected for Malware Assessment.

PLATFORM	DIRECT AGENT	SCOM AGENT	AZURE STORAGE	SCOM REQUIRED?	SCOM AGENT DATA SENT VIA MANAGEMENT GROUP	COLLECTION FREQUENCY
Windows	●	●	✗	✗	●	hourly

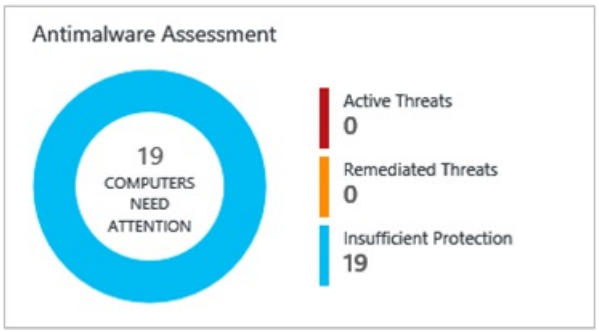
The following table shows examples of data types collected by Malware Assessment:

DATA TYPE	FIELDS
Configuration	CustomerID, AgentID, EntityID, ManagedTypeID, ManagedTypePropertyID, CurrentValue, ChangeDate
Metadata	BaseManagedEntityId, ObjectStatus, OrganizationalUnit, ActiveDirectoryObjectSid, PhysicalProcessors, NetworkName, IPAddress, ForestDNSName, NetbiosComputerName, VirtualMachineName, LastInventoryDate, HostServerNameIsVirtualMachine, IP Address, NetbiosDomainName, LogicalProcessors, DNSName, DisplayName, DomainDnsName, ActiveDirectorySite, PrincipalName, OffsetInMinuteFromGreenwichTime
State	StateChangeEventId, StateId, NewHealthState, OldHealthState, Context, TimeGenerated, TimeAdded, StateId2, BaseManagedEntityId, MonitorId, HealthState, LastModified, LastGreenAlertGenerated, DatabaseTimeModified

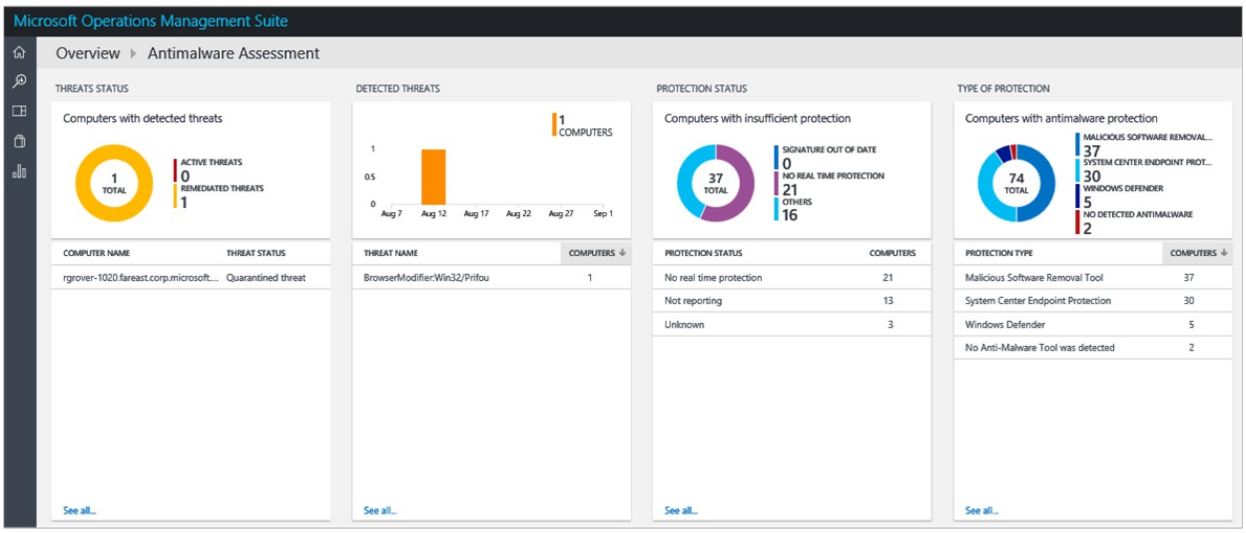
Review threats for servers

When your computers are adequately protected, active threats are quickly quarantined by your antimalware software and should rarely appear as active threats. For that reason, review remediated threats that show the effectiveness of the Antimalware Assessment solution in the following example procedure.

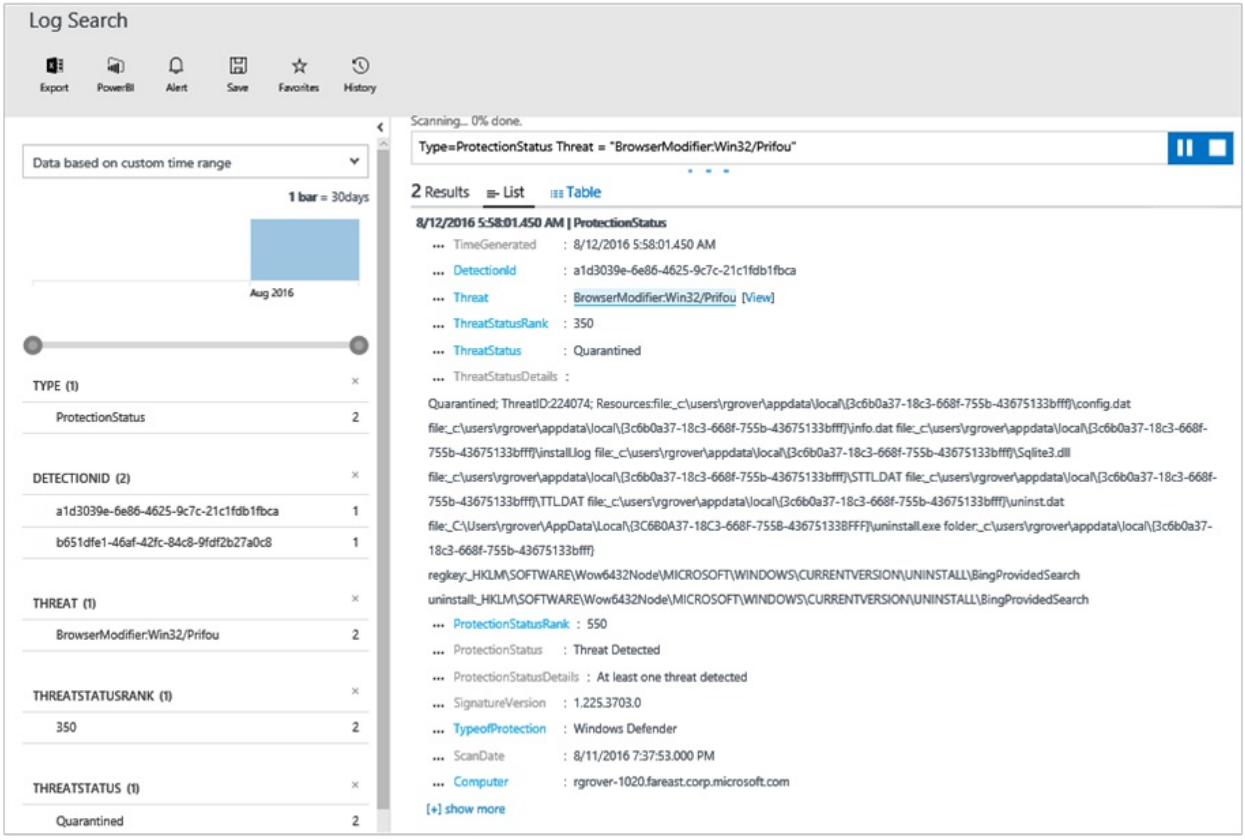
1. On the **Overview** page, click the **Antimalware Assessment** tile.



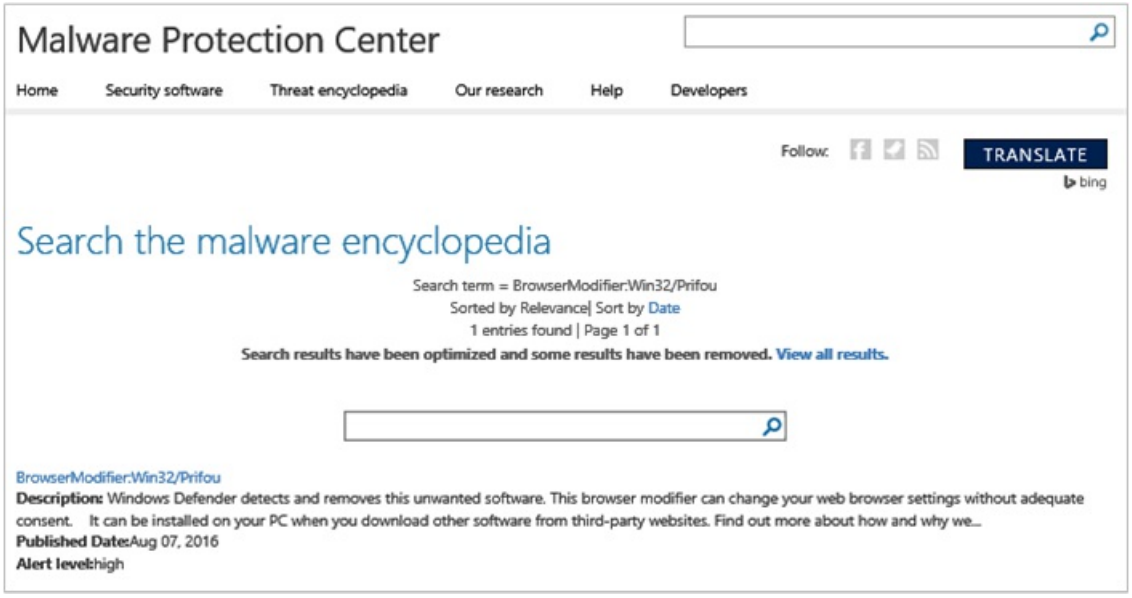
2. On the **Antimalware** dashboard, review the **Detected Threats** blade and click a server name with remediated threats.



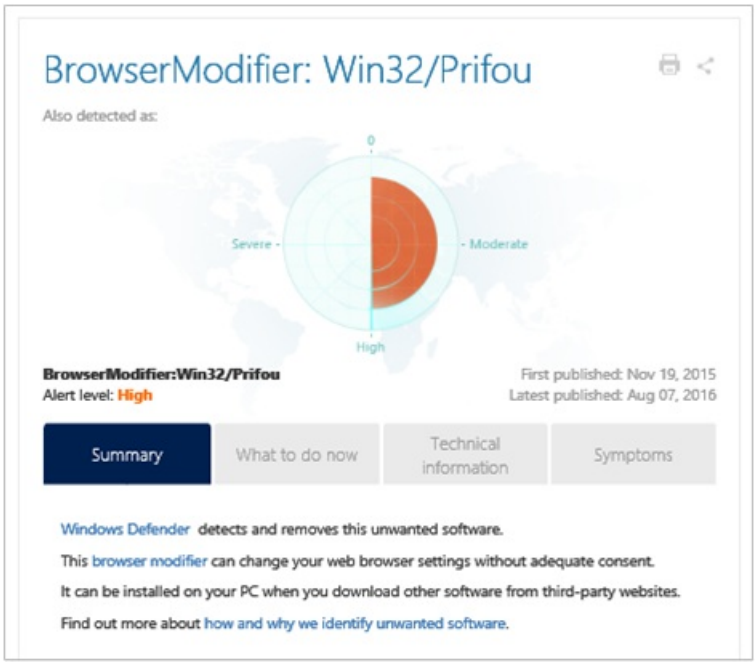
3. On the **Search** page you can see detailed information about the quarantined threat. Next to **Threat**, click **View**.



4. On the **Search the malware encyclopedia** page, click the malware item to view more details about it.

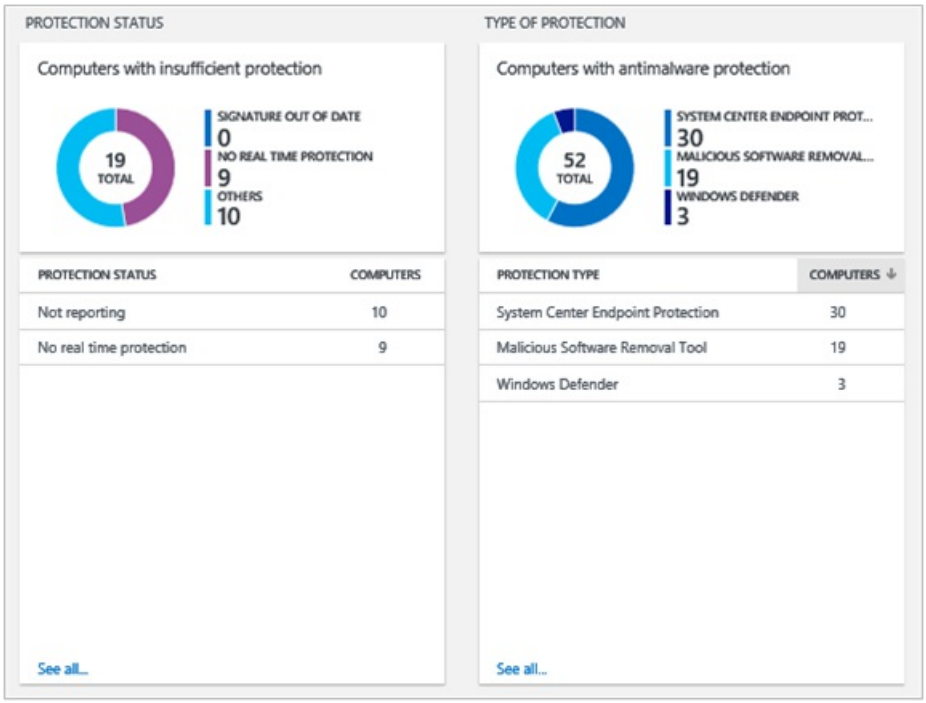


5. On the Microsoft **Malware Protection Center** page for the malware item, review information in the **Summary** section. This section describes how your antimalware software can detect and remove the threat and provides information about what threat the malware might have to your computers.

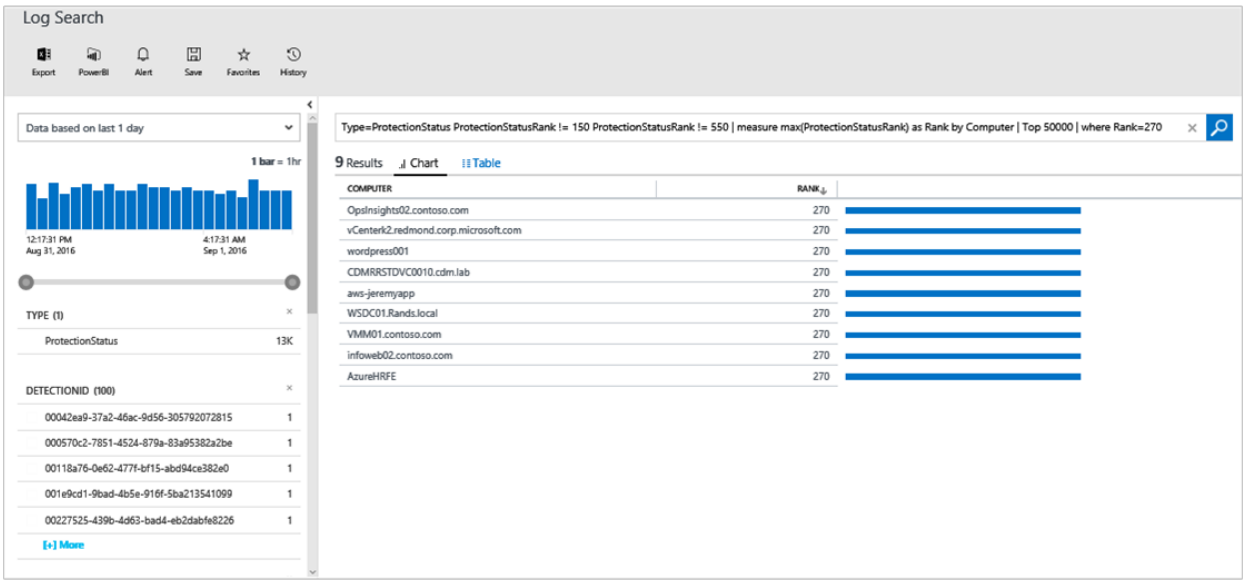


Review protection status

1. On the **Antimalware** dashboard, review the **Protection Status** blade and click **No real time protection**.



2. Search shows a list of servers without protection.



3. Servers without real time protection are displayed.

Computers that do not have supported antimalware software are reported as **No real time protection**.

Next steps

- Use Log searches in Log Analytics to view detailed malware assessment data.

Design and build a management solution in Operations Management Suite (OMS) (Preview)

4/27/2017 • 4 min to read • Edit Online

NOTE

This is preliminary documentation for creating management solutions in OMS which are currently in preview. Any schema described below is subject to change.

Management solutions extend the functionality of Operations Management Suite (OMS) by providing packaged management scenarios that customers can add to their OMS workspace. This article presents a basic process to design and build a management solution that is suitable for most common requirements. If you are new to building management solutions then you can use this process as a starting point and then leverage the concepts for more complex solutions as your requirements evolve.

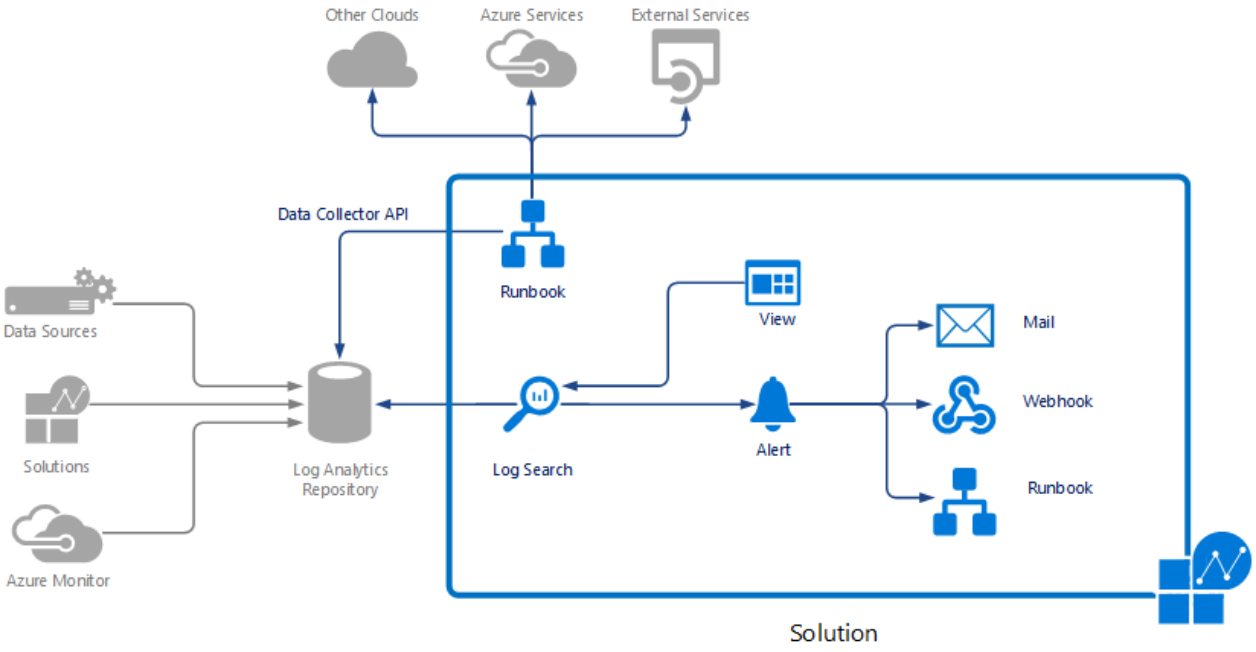
What is a management solution?

Management solutions contain OMS and Azure resources that work together to achieve a particular monitoring scenario. They are implemented as Resource Management templates that contain details of how to install and configure their contained resources when the solution is installed.

The basic strategy is to start your management solution by building the individual components in your Azure environment. Once you have the functionality working properly, then you can start packaging them into a management solution file.

Design your solution

The most common pattern for a management solution is shown in the following diagram. The different components in this pattern are discussed in the below.



Data sources

The first step in designing a solution is determining the data that you require from the Log Analytics repository. This data may be collected by a data source or another solution, or your solution may need to provide the process to collect it.

There are a number of ways data sources that can be collected in the Log Analytics repository as described in Data sources in Log Analytics. This includes events in the Windows Event Log or generated by Syslog in addition to performance counters for both Windows and Linux clients. You can also gather data from Azure resources collected by Azure Monitor.

If you require data that's not accessible through any of the available data sources, then you can use the HTTP Data Collector API which allows you to write data to the Log Analytics repository from any client that can call a REST API. The most common means of custom data collection in a management solution is to create a runbook in Azure Automation that collects the required data from Azure or external resources and uses the Data Collector API to write to the repository.

Log searches

Log searches are used to extract and analyze data in the Log Analytics repository. They are used by views and alerts in addition to allowing the user to perform ad hoc analysis of data in the repository.

You should define any queries that you think will be helpful to the user even if they aren't used by any views or alerts. These will be available to them as Saved Searches in the portal, and you can also include then in a List of Queries visualization part in your custom view.

Alerts

Alerts in Log Analytics identify issues through log searches against the data in the repository. They either notify the user or automatically run an action in response. You should identify different alert conditions for your application and include corresponding alert rules in your solution file.

If the issue can potentially be corrected with an automated process, then you'll typically create a runbook in Azure Automation to perform this remediation. Most Azure services can be managed with cmdlets which the runbook would leverage to perform such functionality.

If your solution requires external functionality in response to an alert, then you can use a webhook response. This allows you to call an external web service sending information from the alert.

Views

Views in Log Analytics are used to visualize data from the Log Analytics repository. Each solution will typically contain a single view with a tile that is displayed on the user's main dashboard. The view can contain any number of visualization parts to provide different visualizations of the collected data to the user.

You create custom views using the View Designer which you can later export for inclusion in your solution file.

Create solution file

Once you've configured and tested the components that will be part of your solution, you can create your solution file. You will implement the solution components in a Resource Manager template that includes a solution resource with relationships to the other resources in the file.

Test your solution

While you are developing your solution, you will need to install and test it in your workspace. You can do this using any of the available methods to test and install Resource Manager templates.

Publish your solution

Once you have completed and tested your solution, you can make it available to customers through either the

following sources.

- **Azure Quickstart templates**. Azure Quickstart templates is a set of Resource Manager templates contributed by the community through GitHub. You can make your solution available by following information in the contribution guide.
- **Azure Marketplace**. The Azure Marketplace allows you to distribute and sell your solution to other developers, ISVs, and IT professionals. You can learn how to publish your solution to Azure Marketplace at How to publish and manage an offer in the Azure Marketplace.

Next steps

- Learn how to create a solution file for your management solution.
- Learn the details of Authoring Azure Resource Manager templates.
- Search Azure Quickstart Templates for samples of different Resource Manager templates.

Creating a management solution file in Operations Management Suite (OMS) (Preview)

5/3/2017 • 7 min to read • Edit Online

> **NOTE**
> This is preliminary documentation for creating management solutions in OMS which are currently in preview. Any schema described below is subject to change.

Management solutions in Operations Management Suite (OMS) are implemented as Resource Manager templates. The main task in learning how to author management solutions is learning how to author a template. This article provides unique details of templates used for solutions and how to configure typical solution resources.

Tools

You can use any text editor to work with solution files, but we recommend leveraging the features provided in Visual Studio or Visual Studio Code as described in the following articles.

- Creating and deploying Azure resource groups through Visual Studio
- Working with Azure Resource Manager Templates in Visual Studio Code

Structure

The basic structure of a management solution file is the same as a Resource Manager Template which is as follows. Each of the sections below describes the top level elements and and their contents in a solution.

```
{
   "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
   "contentVersion": "1.0",
   "parameters": {  },
   "variables": {  },
   "resources": [  ],
   "outputs": {  }
}
```

Parameters

Parameters are values that you require from the user when they install the management solution. There are standard parameters that all solutions will have, and you can add additional parameters as required for your particular solution. How users will provide parameter values when they install your solution will depend on the particular parameter and how the solution is being installed.

When a user installs your management solution through the Azure Marketplace or Azure QuickStart templates they are prompted to select an OMS workspace and Automation account. These are used to populate the values of each of the standard parameters. The user is not prompted to directly provide values for the standard parameters, but they are prompted to provide values for any additional parameters.

When the user installs your solution another method, they must provide a value for all standard parameters and all additional parameters.

A sample parameter is shown below.

```
"startTime": {
    "type": "string",
    "metadata": {
        "description": "Enter time for starting VMs by resource group.",
        "control": "datetime",
        "category": "Schedule"
    }
```

The following table describes the attributes of a parameter.

ATTRIBUTE	DESCRIPTION
type	Data type for the parameter. The input control displayed for the user depends on the data type. bool - Drop down box string - Text box int - Text box securestring - Password field
category	Optional category for the parameter. Parameters in the same category are grouped together.
control	Additional functionality for string parameters. datetime - Datetime control is displayed. guid - Guid value is automatically generated, and the parameter is not displayed.
description	Optional description for the parameter. Displayed in an information balloon next to the parameter.

Standard parameters

The following table lists the standard parameters for all management solutions. These values are populated for the user instead of prompting for them when your solution is installed from the Azure Marketplace or Quickstart templates. The user must provide values for them if the solution is installed with another method.

> **NOTE**
> The user interface in the Azure Marketplace and Quickstart templates is expecting the parameter names in the table. If you use different parameter names then the user will be prompted for them, and they will not be automatically populated.

PARAMETER	TYPE	DESCRIPTION
accountName	string	Azure Automation account name.
pricingTier	string	Pricing tier of both Log Analytics workspace and Azure Automation account.
regionId	string	Region of the Azure Automation account.

PARAMETER	TYPE	DESCRIPTION
solutionName	string	Name of the solution. If you are deploying your solution through Quickstart templates, then you should define solutionName as a parameter so you can define a string instead requiring the user to specify one.
workspaceName	string	Log Analytics workspace name.
workspaceRegionId	string	Region of the Log Analytics workspace.

Sample

Following is a sample parameter entity for a solution. This includes all of the standard parameters and two additional parameters in the same category.

```
"parameters": {
    "workspaceName": {
        "type": "string",
        "metadata": {
            "description": "A valid Log Analytics workspace name"
        }
    },
    "accountName": {
           "type": "string",
           "metadata": {
               "description": "A valid Azure Automation account name"
           }
    },
    "workspaceRegionId": {
           "type": "string",
           "metadata": {
               "description": "Region of the Log Analytics workspace"
        }
    },
    "regionId": {
        "type": "string",
        "metadata": {
            "description": "Region of the Azure Automation account"
        }
    },
    "pricingTier": {
        "type": "string",
        "metadata": {
            "description": "Pricing tier of both Log Analytics workspace and Azure Automation account"
        }
    },
    "jobIdGuid": {
    "type": "string",
        "metadata": {
            "description": "GUID for a runbook job",
            "control": "guid",
            "category": "Schedule"
        }
    },
    "startTime": {
        "type": "string",
        "metadata": {
            "description": "Time for starting the runbook.",
            "control": "datetime",
            "category": "Schedule"
        }
    }
}
```

You refer to parameter values in other elements of the solution with the syntax **parameters('parameter name')**. For example, to access the workspace name, you would use **parameters('workspaceName')**

Variables

Variables are values that you will use in the rest of the management solution. These values are not exposed to the user installing the solution. They are intended to provide the author with a single location where they can manage values that may be used multiple times throughout the solution. You should put any values specific to your solution in variables as opposed to hard coding them in the **resources** element. This makes the code more readable and allows you to easily change these values in later versions.

Following is an example of a **variables** element with typical parameters used in solutions.

```
"variables": {
    "SolutionVersion": "1.1",
    "SolutionPublisher": "Contoso",
    "SolutionName": "My Solution",
    "LogAnalyticsApiVersion": "2015-11-01-preview",
    "AutomationApiVersion": "2015-10-31"
},
```

You refer to variable values through the solution with the syntax **variables('variable name')**. For example, to access the SolutionName variable, you would use **variables('SolutionName')**.

You can also define complex variables that multiple sets of values. These are particularly useful in management solutions where you are defining multiple properties for different types of resources. For example, you could restructure the solution variables shown above to the following.

```
"variables": {
    "Solution": {
      "Version": "1.1",
      "Publisher": "Contoso",
      "Name": "My Solution"
    },
    "LogAnalyticsApiVersion": "2015-11-01-preview",
    "AutomationApiVersion": "2015-10-31"
},
```

In this case, you refer to variable values through the solution with the syntax **variables('variable name').property**. For example, to access the Solution Name variable, you would use **variables('Solution').Name**.

Resources

Resources define the different resources that your management solution will install and configure. This will be the largest and most complex portion of the template. You can get the structure and complete description of resource elements in Authoring Azure Resource Manager templates. Different resources that you will typically define are detailed in other articles in this documentation.

Dependencies

The **dependsOn** elements specifies a dependency on another resource. When the solution is installed, a resource is not created until all of its dependencies have been created. For example, your solution might start a runbook when it's installed using a job resource. The job resource would be dependent on the runbook resource to make sure that the runbook is created before the job is created.

OMS workspace and Automation account

Management solutions require an OMS workspace to contain views and an Automation account to contain runbooks and related resources. These must be available before the resources in the solution are created and should not be defined in the solution itself. The user will specify a workspace and account when they deploy your solution, but as the author you should consider the following points.

Solution resource

Each solution requires a resource entry in the **resources** element that defines the solution itself. This will have a type of **Microsoft.OperationsManagement/solutions** and have the following structure. This includes standard parameters and variables that are typically used to define properties of the solution.

```
{
  "name": "[concat(variables('Solution').Name, '[' ,parameters('workspacename'), ']')]",
  "location": "[parameters('workspaceRegionId')]",
  "tags": { },
  "type": "Microsoft.OperationsManagement/solutions",
  "apiVersion": "[variables('LogAnalyticsApiVersion')]",
  "dependsOn": [
    <list-of-resources>
  ],
  "properties": {
    "workspaceResourceId": "[resourceId('Microsoft.OperationalInsights/workspaces',
parameters('workspacename'))]",
    "referencedResources": [
        <list-of-referenced-resources>
    ],
    "containedResources": [
        <list-of-contained-resources>
    ]
  },
  "plan": {
    "name": "[concat(variables('Solution').Name, '[' ,parameters('workspaceName'), ']')]",
    "Version": "[variables('Solution').Version]",
    "product": "[variables('ProductName')]",
    "publisher": "[variables('Solution').Publisher]",
    "promotionCode": ""
  }
}
```

Dependencies

The solution resource must have a dependency on every other resource in the solution since they need to exist before the solution can be created. You do this by adding an entry for each resource in the **dependsOn** element.

Properties

The solution resource has the properties in the following table. This includes the resources referenced and contained by the solution which defines how the resource is managed after the solution is installed. Each resource in the solution should be listed in either the **referencedResources** or the **containedResources** property.

PROPERTY	DESCRIPTION
workspaceResourceId	ID of the Log Analytics workspace in the form */providers/Microsoft.OperationalInsights/workspaces/<Workspace Name>*.
referencedResources	List of resources in the solution that should not be removed when the solution is removed.
containedResources	List of resources in the solution that should be removed when the solution is removed.

The example above is for a solution with a runbook, a schedule, and view. The schedule and runbook are *referenced* in the **properties** element so they are not removed when the solution is removed. The view is *contained* so it is removed when the solution is removed.

Plan

The **plan** entity of the solution resource has the properties in the following table.

PROPERTY	DESCRIPTION
name	Name of the solution.
version	Version of the solution as determined by the author.
product	Unique string to identify the solution.
publisher	Publisher of the solution.

Sample

You can view samples of solution files with a solution resource at the following locations.

- Automation resources
- Search and alert resources

Next steps

- Add saved searches and alerts to your management solution.
- Add views to your management solution.
- Add runbooks and other Automation resources to your management solution.
- Learn the details of Authoring Azure Resource Manager templates.
- Search Azure Quickstart Templates for samples of different Resource Manager templates.

Adding Azure Automation resources to an OMS management solution (Preview)

3/21/2017 • 11 min to read • Edit Online

> **NOTE**
> This is preliminary documentation for creating management solutions in OMS which are currently in preview. Any schema described below is subject to change.

Management solutions in OMS will typically include runbooks in Azure Automation to automate processes such as collecting and processing monitoring data. In addition to runbooks, Automation accounts includes assets such as variables and schedules that support the runbooks used in the solution. This article describes how to include runbooks and their related resources in a solution.

> **NOTE**
> The samples in this article use parameters and variables that are either required or common to management solutions and described in Creating management solutions in Operations Management Suite (OMS)

Prerequisites

This article assumes that you're already familiar with the following information.

- How to create a management solution.
- The structure of a solution file.
- How to author Resource Manager templates

Automation account

All resources in Azure Automation are contained in an Automation account. As described in OMS workspace and Automation account the Automation account isn't included in the management solution but must exist before the solution is installed. If it isn't available, then the solution install will fail.

The name of each Automation resource includes the name of its Automation account. This is done in the solution with the **accountName** parameter as in the following example of a runbook resource.

```
"name": "[concat(parameters('accountName'), '/MyRunbook'))]"
```

Runbooks

You should include any runbooks used by the solution in the solution file so that they're created when the solution is installed. You cannot contain the body of the runbook in the template though, so you should publish the runbook to a public location where it can be accessed by any user installing your solution.

Azure Automation runbook resources have a type of **Microsoft.Automation/automationAccounts/runbooks** and have the following structure. This includes common variables and parameters so that you can copy and paste this code snippet into your solution file and change the parameter names.

```
{
    "name": "[concat(parameters('accountName'), '/', variables('Runbook').Name)]",
    "type": "Microsoft.Automation/automationAccounts/runbooks",
    "apiVersion": "[variables('AutomationApiVersion')]",
    "dependsOn": [
    ],
    "location": "[parameters('regionId')]",
    "tags": { },
    "properties": {
        "runbookType": "[variables('Runbook').Type]",
        "logProgress": "true",
        "logVerbose": "true",
        "description": "[variables('Runbook').Description]",
        "publishContentLink": {
            "uri": "[variables('Runbook').Uri]",
            "version": [variables('Runbook').Version]"
        }
    }
}
```

The properties for runbooks are described in the following table.

PROPERTY	DESCRIPTION
runbookType	Specifies the types of the runbook. Script - PowerShell script PowerShell - PowerShell workflow GraphPowerShell - Graphical PowerShell script runbook GraphPowerShellWorkflow - Graphical PowerShell workflow runbook
logProgress	Specifies whether progress records should be generated for the runbook.
logVerbose	Specifies whether verbose records should be generated for the runbook.
description	Optional description for the runbook.
publishContentLink	Specifies the content of the runbook. uri - Uri to the content of the runbook. This will be a .ps1 file for PowerShell and Script runbooks, and an exported graphical runbook file for a Graph runbook. version - Version of the runbook for your own tracking.

Automation jobs

When you start a runbook in Azure Automation, it creates an automation job. You can add an automation job resource to your solution to automatically start a runbook when the management solution is installed. This method is typically used to start runbooks that are used for initial configuration of the solution. To start a runbook at regular intervals, create a schedule and a job schedule

Job resources have a type of **Microsoft.Automation/automationAccounts/jobs** and have the following structure. This includes common variables and parameters so that you can copy and paste this code snippet into your solution file and change the parameter names.

```
{
  "name": "[concat(parameters('accountName'), '/', parameters('Runbook').JobGuid)]",
  "type": "Microsoft.Automation/automationAccounts/jobs",
  "apiVersion": "[variables('AutomationApiVersion')]",
  "location": "[parameters('regionId')]",
  "dependsOn": [
    "[concat('Microsoft.Automation/automationAccounts/', parameters('accountName'), '/runbooks/',
variables('Runbook').Name)]"
  ],
  "tags": { },
  "properties": {
    "runbook": {
      "name": "[variables('Runbook').Name]"
    },
    "parameters": {
      "Parameter1": "[[variables('Runbook').Parameter1]",
      "Parameter2": "[[variables('Runbook').Parameter2]"
    }
  }
}
```

The properties for automation jobs are described in the following table.

PROPERTY	DESCRIPTION
runbook	Single name entity with the name of the runbook to start.
parameters	Entity for each parameter value required by the runbook.

The job includes the runbook name and any parameter values to be sent to the runbook. The job should depend on the runbook that it's starting since the runbook must be created before the job. If you have multiple runbooks that should be started you can define their order by having a job depend on any other jobs that should be run first.

The name of a job resource must contain a GUID which is typically assigned by a parameter. You can read more about GUID parameters in Creating solutions in Operations Management Suite (OMS).

Certificates

Azure Automation certificates have a type of **Microsoft.Automation/automationAccounts/certificates** and have the following structure. This includes common variables and parameters so that you can copy and paste this code snippet into your solution file and change the parameter names.

```
{
  "name": "[concat(parameters('accountName'), '/', variables('Certificate').Name)]",
  "type": "Microsoft.Automation/automationAccounts/certificates",
  "apiVersion": "[variables('AutomationApiVersion')]",
  "location": "[parameters('regionId')]",
  "tags": { },
  "dependsOn": [
  ],
  "properties": {
    "base64Value": "[variables('Certificate').Base64Value]",
    "thumbprint": "[variables('Certificate').Thumbprint]"
  }
}
```

The properties for Certificates resources are described in the following table.

PROPERTY	DESCRIPTION
base64Value	Base 64 value for the certificate.
thumbprint	Thumbprint for the certificate.

Credentials

Azure Automation credentials have a type of **Microsoft.Automation/automationAccounts/credentials** and have the following structure. This includes common variables and parameters so that you can copy and paste this code snippet into your solution file and change the parameter names.

```
{
  "name": "[concat(parameters('accountName'), '/', variables('Credential').Name)]",
  "type": "Microsoft.Automation/automationAccounts/credentials",
  "apiVersion": "[variables('AutomationApiVersion')]",
  "location": "[parameters('regionId')]",
  "tags": { },
  "dependsOn": [
  ],
  "properties": {
    "userName": "[parameters('credentialUsername')]",
    "password": "[parameters('credentialPassword')]"
  }
}
```

The properties for Credential resources are described in the following table.

PROPERTY	DESCRIPTION
userName	User name for the credential.
password	Password for the credential.

Schedules

Azure Automation schedules have a type of **Microsoft.Automation/automationAccounts/schedules** and have the the following structure. This includes common variables and parameters so that you can copy and paste this code snippet into your solution file and change the parameter names.

```
{
  "name": "[concat(parameters('accountName'), '/', variables('Schedule').Name)]",
  "type": "microsoft.automation/automationAccounts/schedules",
  "apiVersion": "[variables('AutomationApiVersion')]",
  "tags": { },
  "dependsOn": [
  ],
  "properties": {
    "description": "[variables('Schedule').Description]",
    "startTime": "[parameters('scheduleStartTime')]",
    "timeZone": "[parameters('scheduleTimeZone')]",
    "isEnabled": "[variables('Schedule').IsEnabled]",
    "interval": "[variables('Schedule').Interval]",
    "frequency": "[variables('Schedule').Frequency]"
  }
}
```

The properties for schedule resources are described in the following table.

PROPERTY	DESCRIPTION
description	Optional description for the schedule.
startTime	Specifies the start time of a schedule as a DateTime object. A string can be provided if it can be converted to a valid DateTime.
isEnabled	Specifies whether the schedule is enabled.
interval	The type of interval for the schedule. day hour
frequency	Frequency that the schedule should fire in number of days or hours.

Schedules must have a start time with a value greater than the current time. You cannot provide this value with a variable since you would have no way of knowing when it's going to be installed.

Use one of the following two strategies when using schedule resources in a solution.

- Use a parameter for the start time of the schedule. This will prompt the user to provide a value when they install the solution. If you have multiple schedules, you could use a single parameter value for more than one of them.
- Create the schedules using a runbook that starts when the solution is installed. This removes the requirement of the user to specify a time, but you can't contain the schedule in your solution so it will be removed when the solution is removed.

Job schedules

Job schedule resources link a runbook with a schedule. They have a type of **Microsoft.Automation/automationAccounts/jobSchedules** and have the the following structure. This includes common variables and parameters so that you can copy and paste this code snippet into your solution file and change the parameter names.

```
{
  "name": "[concat(parameters('accountName'), '/', variables('Schedule').LinkGuid)]",
  "type": "microsoft.automation/automationAccounts/jobSchedules",
  "apiVersion": "[variables('AutomationApiVersion')]",
  "location": "[parameters('regionId')]",
  "dependsOn": [
    "[resourceId('Microsoft.Automation/automationAccounts/runbooks/', parameters('accountName'),
variables('Runbook').Name)]",
    "[resourceId('Microsoft.Automation/automationAccounts/schedules/', parameters('accountName'),
variables('Schedule').Name)]"
  ],
  "tags": {
  },
  "properties": {
    "schedule": {
      "name": "[variables('Schedule').Name]"
    },
    "runbook": {
      "name": "[variables('Runbook').Name]"
    }
  }
}
```

The properties for job schedules are described in the following table.

PROPERTY	DESCRIPTION
schedule name	Single **name** entity with the name of the schedule.
runbook name	Single **name** entity with the name of the runbook.

Variables

Azure Automation variables have a type of **Microsoft.Automation/automationAccounts/variables** and have the following structure. This includes common variables and parameters so that you can copy and paste this code snippet into your solution file and change the parameter names.

```
{
  "name": "[concat(parameters('accountName'), '/', variables('Variable').Name)]",
  "type": "microsoft.automation/automationAccounts/variables",
  "apiVersion": "[variables('AutomationApiVersion')]",
  "tags": { },
  "dependsOn": [
  ],
  "properties": {
    "description": "[variables('Variable').Description]",
    "isEncrypted": "[variables('Variable').Encrypted]",
    "type": "[variables('Variable').Type]",
    "value": "[variables('Variable').Value]"
  }
}
```

The properties for variable resources are described in the following table.

PROPERTY	DESCRIPTION
description	Optional description for the variable.
isEncrypted	Specifies whether the variable should be encrypted.
type	Data type for the variable.
value	Value for the variable.

Modules

Your management solution does not need to define global modules used by your runbooks because they will always be available in your Automation account. You do need to include a resource for any other module used by your runbooks.

Integration modules have a type of **Microsoft.Automation/automationAccounts/modules** and have the following structure. This includes common variables and parameters so that you can copy and paste this code snippet into your solution file and change the parameter names.

```
{
  "name": "[concat(parameters('accountName'), '/', variables('Module').Name)]",
  "type": "Microsoft.Automation/automationAccounts/modules",
  "apiVersion": "[variables('AutomationApiVersion')]",
  "dependsOn": [
  ],
  "properties": {
    "contentLink": {
      "uri": "[variables('Module').Uri]"
    }
  }
}
```

The properties for module resources are described in the following table.

PROPERTY	DESCRIPTION
contentLink	Specifies the content of the module. uri - Uri to the content of the module. This will be a .ps1 file for PowerShell and Script runbooks, and an exported graphical runbook file for a Graph runbook. version - Version of the module for your own tracking.

The runbook should depend on the module resource to ensure that it's created before the runbook.

Updating modules

If you update a management solution that includes a runbook that uses a schedule, and the new version of your solution has a new module used by that runbook, then the runbook may use the old version of the module. You should include the following runbooks in your solution and create a job to run them before any other runbooks. This will ensure that any modules are updated as required before the runbooks are loaded.

- Update-ModulesinAutomationToLatestVersion will ensure that all of the modules used by runbooks in your solution are the latest version.
- ReRegisterAutomationSchedule-MS-Mgmt will reregister all of the schedule resources to ensure that the runbooks linked to them with use the latest modules.

Sample

Following is a sample of a solution that include that includes the following resources:

- Runbook. This is a sample runbook stored in a public GitHub repository.
- Automation job that starts the runbook when the solution is installed.
- Schedule and job schedule to start the runbook at regular intervals.
- Certificate.
- Credential.
- Variable.
- Module. This is the OMSIngestionAPI module for writing data to Log Analytics.

The sample uses standard solution parameters variables that would commonly be used in a solution as opposed to hardcoding values in the resource definitions.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "workspaceName": {
```

```
      "type": "string",
      "metadata": {
        "Description": "Name of Log Analytics workspace."
      }
    },
    "accountName": {
      "type": "string",
      "metadata": {
        "Description": "Name of Automation account."
      }
    },
    "workspaceregionId": {
      "type": "string",
      "metadata": {
        "Description": "Region of Log Analytics workspace."
      }
    },
    "regionId": {
      "type": "string",
      "metadata": {
        "Description": "Region of Automation account."
      }
    },
    "pricingTier": {
      "type": "string",
      "metadata": {
        "Description": "Pricing tier of both Log Analytics workspace and Azure Automation account."
      }
    },
    "certificateBase64Value": {
      "type": "string",
      "metadata": {
        "Description": "Base 64 value for certificate."
      }
    },
    "certificateThumbprint": {
      "type": "securestring",
      "metadata": {
        "Description": "Thumbprint for certificate."
      }
    },
    "credentialUsername": {
      "type": "string",
      "metadata": {
        "Description": "Username for credential."
      }
    },
    "credentialPassword": {
      "type": "securestring",
      "metadata": {
        "Description": "Password for credential."
      }
    },
    "scheduleStartTime": {
      "type": "string",
      "metadata": {
        "Description": "Start time for shedule."
      }
    },
    "scheduleTimeZone": {
      "type": "string",
      "metadata": {
        "Description": "Time zone for schedule."
      }
    },
    "scheduleLinkGuid": {
      "type": "string",
      "metadata": {
        "description": "GUID for the schedule link to runbook.",
```

```
        "control": "guid"
      }
    },
    "runbookJobGuid": {
      "type": "string",
      "metadata": {
        "description": "GUID for the runbook job.",
        "control": "guid"
      }
    }
  },
  "variables": {
    "SolutionName": "MySolution",
    "SolutionVersion": "1.0",
    "SolutionPublisher": "Contoso",
    "ProductName": "SampleSolution",

    "LogAnalyticsApiVersion": "2015-11-01-preview",
    "AutomationApiVersion": "2015-10-31",

    "Runbook": {
      "Name": "MyRunbook",
      "Description": "Sample runbook",
      "Type": "PowerShell",
      "Uri": "https://raw.githubusercontent.com/user/myrepo/master/samples/MyRunbook.ps1",
      "JobGuid": "[parameters('runbookJobGuid')]"
    },

    "Certificate": {
      "Name": "MyCertificate",
      "Base64Value": "[parameters('certificateBase64Value')]",
      "Thumbprint": "[parameters('certificateThumbprint')]"
    },

    "Credential": {
      "Name": "MyCredential",
      "UserName": "[parameters('credentialUsername')]",
      "Password": "[parameters('credentialPassword')]"
    },

    "Schedule": {
      "Name": "MySchedule",
      "Description": "Sample schedule",
      "IsEnabled": "true",
      "Interval": "1",
      "Frequency": "hour",
      "StartTime": "[parameters('scheduleStartTime')]",
      "TimeZone": "[parameters('scheduleTimeZone')]",
      "LinkGuid": "[parameters('scheduleLinkGuid')]"
    },

    "Variable": {
      "Name": "MyVariable",
      "Description": "Sample variable",
      "Encrypted": 0,
      "Type": "string",
      "Value": "'This is my string value.'"
    },

    "Module": {
      "Name": "OMSIngestionAPI",
      "Uri": "https://devopsgallerystorage.blob.core.windows.net/packages/omsingestionapi.1.3.0.nupkg"
    }
  },
  "resources": [
    {
      "name": "[concat(variables('SolutionName'), '[' ,parameters('workspacename'), ']')]",
      "location": "[parameters('workspaceRegionId')]",
      "tags": { },
```

```
      "type": "Microsoft.OperationsManagement/solutions",
      "apiVersion": "[variables('LogAnalyticsApiVersion')]",
      "dependsOn": [
        "[resourceId('Microsoft.Automation/automationAccounts/runbooks/', parameters('accountName'),
variables('Runbook').Name)]",
        "[resourceId('Microsoft.Automation/automationAccounts/jobs/', parameters('accountName'),
variables('Runbook').JobGuid)]",
        "[resourceId('Microsoft.Automation/automationAccounts/certificates/', parameters('accountName'),
variables('Certificate').Name)]",
        "[resourceId('Microsoft.Automation/automationAccounts/credentials/', parameters('accountName'),
variables('Credential').Name)]",
        "[resourceId('Microsoft.Automation/automationAccounts/schedules/', parameters('accountName'),
variables('Schedule').Name)]",
        "[resourceId('Microsoft.Automation/automationAccounts/jobSchedules/', parameters('accountName'),
variables('Schedule').LinkGuid)]",
        "[resourceId('Microsoft.Automation/automationAccounts/variables/', parameters('accountName'),
variables('Variable').Name)]",
        "[resourceId('Microsoft.Automation/automationAccounts/modules/', parameters('accountName'),
variables('Module').Name)]"
      ],
      "properties": {
        "workspaceResourceId": "[resourceId('Microsoft.OperationalInsights/workspaces',
parameters('workspacename'))]",
        "referencedResources": [
          "[resourceId('Microsoft.Automation/automationAccounts/modules/', parameters('accountName'),
variables('Module').Name)]"
        ],
        "containedResources": [
          "[resourceId('Microsoft.Automation/automationAccounts/runbooks/', parameters('accountName'),
variables('Runbook').Name)]",
          "[resourceId('Microsoft.Automation/automationAccounts/jobs/', parameters('accountName'),
variables('Runbook').JobGuid)]",
          "[resourceId('Microsoft.Automation/automationAccounts/certificates/', parameters('accountName'),
variables('Certificate').Name)]",
          "[resourceId('Microsoft.Automation/automationAccounts/credentials/', parameters('accountName'),
variables('Credential').Name)]",
          "[resourceId('Microsoft.Automation/automationAccounts/schedules/', parameters('accountName'),
variables('Schedule').Name)]",
          "[resourceId('Microsoft.Automation/automationAccounts/jobSchedules/', parameters('accountName'),
variables('Schedule').LinkGuid)]",
          "[resourceId('Microsoft.Automation/automationAccounts/variables/', parameters('accountName'),
variables('Variable').Name)]"
        ]
      },
      "plan": {
        "name": "[concat(variables('SolutionName'), '[' ,parameters('workspaceName'), ']')]",
        "Version": "[variables('SolutionVersion')]",
        "product": "[variables('ProductName')]",
        "publisher": "[variables('SolutionPublisher')]",
        "promotionCode": ""
      }
    },
    {
      "name": "[concat(parameters('accountName'), '/', variables('Runbook').Name)]",
      "type": "Microsoft.Automation/automationAccounts/runbooks",
      "apiVersion": "[variables('AutomationApiVersion')]",
      "dependsOn": [
      ],
      "location": "[parameters('regionId')]",
      "tags": { },
      "properties": {
        "runbookType": "[variables('Runbook').Type]",
        "logProgress": "true",
        "logVerbose": "true",
        "description": "[variables('Runbook').Description]",
        "publishContentLink": {
          "uri": "[variables('Runbook').Uri]",
          "version": "1.0.0.0"
        }
```

```
      }
    },
    {
      "name": "[concat(parameters('accountName'), '/', variables('Runbook').JobGuid)]",
      "type": "Microsoft.Automation/automationAccounts/jobs",
      "apiVersion": "[variables('AutomationApiVersion')]",
      "location": "[parameters('regionId')]",
      "dependsOn": [
        "[concat('Microsoft.Automation/automationAccounts/', parameters('accountName'), '/runbooks/',
variables('Runbook').Name)]"
      ],
      "tags": { },
      "properties": {
        "runbook": {
          "name": "[variables('Runbook').Name]"
        },
        "parameters": {
          "targetSubscriptionId": "[subscription().subscriptionId]",
          "resourcegroup": "[resourceGroup().name]",
          "automationaccount": "[parameters('accountName')]"
        }
      }
    },
    {
      "name": "[concat(parameters('accountName'), '/', variables('Certificate').Name)]",
      "type": "Microsoft.Automation/automationAccounts/certificates",
      "apiVersion": "[variables('AutomationApiVersion')]",
      "location": "[parameters('regionId')]",
      "tags": { },
      "dependsOn": [
      ],
      "properties": {
        "Base64Value": "[variables('Certificate').Base64Value]",
        "Thumbprint": "[variables('Certificate').Thumbprint]"
      }
    },
    {
      "name": "[concat(parameters('accountName'), '/', variables('Credential').Name)]",
      "type": "Microsoft.Automation/automationAccounts/credentials",
      "apiVersion": "[variables('AutomationApiVersion')]",
      "location": "[parameters('regionId')]",
      "tags": { },
      "dependsOn": [
      ],
      "properties": {
        "userName": "[variables('Credential').UserName]",
        "password": "[variables('Credential').Password]"
      }
    },
    {
      "name": "[concat(parameters('accountName'), '/', variables('Schedule').Name)]",
      "type": "microsoft.automation/automationAccounts/schedules",
      "apiVersion": "[variables('AutomationApiVersion')]",
      "tags": { },
      "dependsOn": [
      ],
      "properties": {
        "description": "[variables('Schedule').Description]",
        "startTime": "[variables('Schedule').StartTime]",
        "timeZone": "[variables('Schedule').TimeZone]",
        "isEnabled": "[variables('Schedule').IsEnabled]",
        "interval": "[variables('Schedule').Interval]",
        "frequency": "[variables('Schedule').Frequency]"
      }
    },
    {
      "name": "[concat(parameters('accountName'), '/', variables('Schedule').LinkGuid)]",
      "type": "microsoft.automation/automationAccounts/jobSchedules",
      "apiVersion": "[variables('AutomationApiVersion')]"
```

```
      "apiVersion": "[variables('AutomationApiVersion')]",
      "location": "[parameters('regionId')]",
      "dependsOn": [
        "[resourceId('Microsoft.Automation/automationAccounts/runbooks/', parameters('accountName'),
variables('Runbook').Name)]",
        "[resourceId('Microsoft.Automation/automationAccounts/schedules/', parameters('accountName'),
variables('Schedule').Name)]"
      ],
      "tags": {
      },
      "properties": {
        "schedule": {
          "name": "[variables('Schedule').Name]"
        },
        "runbook": {
          "name": "[variables('Runbook').Name]"
        }
      }
    },
    {
      "name": "[concat(parameters('accountName'), '/', variables('Variable').Name)]",
      "type": "microsoft.automation/automationAccounts/variables",
      "apiVersion": "[variables('AutomationApiVersion')]",
      "tags": { },
      "dependsOn": [
      ],
      "properties": {
        "description": "[variables('Variable').Description]",
        "isEncrypted": "[variables('Variable').Encrypted]",
        "type": "[variables('Variable').Type]",
        "value": "[variables('Variable').Value]"
      }
    },
    {
      "name": "[concat(parameters('accountName'), '/', variables('Module').Name)]",
      "type": "Microsoft.Automation/automationAccounts/modules",
      "apiVersion": "[variables('AutomationApiVersion')]",
      "dependsOn": [
      ],
      "properties": {
        "contentLink": {
          "uri": "[variables('Module').Uri]"
        }
      }
    }

  ],
  "outputs": { }
}
```

Next steps

- Add a view to your solution to visualize collected data.

Adding Log Analytics saved searches and alerts to OMS management solution (Preview)

4/12/2017 • 9 min to read • Edit Online

> **NOTE**
> This is preliminary documentation for creating management solutions in OMS which are currently in preview. Any schema described below is subject to change.

Management solutions in OMS will typically include saved searches in Log Analytics to analyze data collected by the solution. They may also define alerts to notify the user or automatically take action in response to a critical issue. This article describes how to define Log Analytics saved searches and alerts in a Resource Management template so they can be included in management solutions.

> **NOTE**
> The samples in this article use parameters and variables that are either required or common to management solutions and described in Creating management solutions in Operations Management Suite (OMS)

Prerequisites

This article assumes that you're already familiar with how to create a management solution and the structure of an ARM template and solution file.

Log Analytics Workspace

All resources in Log Analytics are contained in a workspace. As described in OMS workspace and Automation account the workspace isn't included in the management solution but must exist before the solution is installed. If it isn't available, then the solution install will fail.

The name of the workspace is in the name of each Log Analytics resource. This is done in the solution with the **workspace** parameter as in the following example of a savedsearch resource.

```
"name": "[concat(parameters('workspaceName'), '/', variables('SavedSearchId'))]"
```

Saved Searches

Include saved searches in a solution to allow users to query data collected by your solution. Saved searches will appear under **Favorites** in the OMS portal and **Saved Searches** in the Azure portal . A saved search is also required for each alert.

Log Analytics saved search resources have a type of `Microsoft.OperationalInsights/workspaces/savedSearches` and have the following structure.

```
{
    "name": "<name-of-savedsearch>"
    "type": "Microsoft.OperationalInsights/workspaces/savedSearches",
    "apiVersion": "<api-version-of-resource>",
    "dependsOn": []
    "tags": {},
    "properties": {
        "etag": "*",
        "query": "<query-to-run>",
        "displayName": "<saved-search-display-name>",
        "category": ""<saved-search-category>"
    }
}
```

Each of the properties of a saved search are described in the following table.

PROPERTY	DESCRIPTION
category	The category for the saved search. Any saved searches in the same solution will often share a single category so they are grouped together in the console.
displayname	Name to display for the saved search in the portal.
query	Query to run.

NOTE

You may need to use escape characters in the query if it includes characters that could be interpreted as JSON. For example, if your query was **Type:AzureActivity OperationName:"Microsoft.Compute/virtualMachines/write"**, it should be written in the solution file as **Type:AzureActivity OperationName:\"Microsoft.Compute/virtualMachines/write\"**.

Alerts

Log Analytics alerts are created by alert rules that run a saved search on a regular interval. If the results of the query match specified criteria, an alert record is created and one or more actions are run.

Alert rules in a management solution are made up of the following three different resources.

- **Saved search.** Defines the log search that will be run. Multiple alert rules can share a single saved search.
- **Schedule.** Defines how often the log search will be run. Each alert rule will have one and only one schedule.
- **Alert action.** Each alert rule will have one action resource with a type of **Alert** that defines the details of the alert such as the criteria for when an alert record will be created and the alert's severity. The action resource will optionally define a mail and runbook response.
- **Webhook action (optional).** If the alert rule will call a webhook, then it requires an additional action resource with a type of **Webhook**.

Saved search resources are described above. The other resources are described below.

Schedule resource

A saved search can have one or more schedules with each schedule representing a separate alert rule. The schedule defines how often the search is run and the time interval over which the data is retrieved. Schedule resources have a type of `Microsoft.OperationalInsights/workspaces/savedSearches/schedules/` and have the following structure.

```
{
  "name": "<name-of-schedule-resource>",
  "type": "Microsoft.OperationalInsights/workspaces/savedSearches/schedules/",
  "apiVersion": "<api-version-of-resource>",
  "dependsOn": [
    "<name-of-saved-search>"
  ],
  "properties": {
    "etag": "*",
    "interval": <schedule-interval-in-minutes>,
    "queryTimeSpan": <query-timespan-in-minutes>,
    "enabled": <schedule-enabled>
  }
}
```

The properties for schedule resources are described in the following table.

ELEMENT NAME	REQUIRED	DESCRIPTION
enabled	Yes	Specifies whether the alert is enabled when it's created.
interval	Yes	How often the query runs in minutes.
queryTimeSpan	Yes	Length of time in minutes over which to evaluate results.

The schedule resource should depend on the saved search so that it's created before the schedule.

Actions

There are two types of action resource specified by the **Type** property. A schedule requires one **Alert** action which defines the details of the alert rule and what actions are taken when an alert is created. It may also include a **Webhook** action if a webhook should be called from the alert.

Action resources have a type of `Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions`.

Alert actions

Every schedule will have one **Alert** action. This defines the details of the alert and optionally notification and remediation actions. A notification sends an email to one or more addresses. A remediation starts a runbook in Azure Automation to attempt to remediate the detected issue.

Alert actions have the following structure.

```
{
    "name": "<name-of-the-action>",
    "type": "Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions",
    "apiVersion": "<api-version-of-resource>",
    "dependsOn": [
        <name-of-schedule>
    ],
    "properties": {
        "etag": "*",
        "type": "Alert",
        "name": "<display-name-of-alert>",
        "description": "<description-of-alert>",
        "severity": "<severity-of-alert>",
        "threshold": {
            "operator": "<threshold-operator>",
            "value": "<threshold-value>"
            "metricsTrigger": {
                "triggerCondition": "<trigger-condition>",
                "operator": "<trigger-operator>",
                "value": "<trigger-value>"
            },
        },
        "throttling": {
            "durationInMinutes": "<throttling-duration-in-minutes>"
        },
        "emailNotification": {
            "recipients": [
                <mail-recipients>
            ],
            "subject": "<mail-subject>",
            "attachment": "None"
        },
        "remediation": {
            "runbookName": "<name-of-runbook>",
            "webhookUri": "<runbook-uri>"
        }
    }
}
```

The properties for Alert action resources are described in the following tables.

ELEMENT NAME	REQUIRED	DESCRIPTION
Type	Yes	Type of the action. This will be **Alert** for alert actions.
Name	Yes	Display name for the alert. This is the name that's displayed in the console for the alert rule.
Description	No	Optional description of the alert.
Severity	Yes	Severity of the alert record from the following values: **Critical** **Warning** **Informational**

Threshold

This section is required. It defines the properties for the alert threshold.

ELEMENT NAME	REQUIRED	DESCRIPTION
Operator	Yes	Operator for the comparison from the following values: **gt = greater than** **lt = less than**
Value	Yes	The value to compare the results.

MetricsTrigger

This section is optional. Include it for a metric measurement alert.

> **NOTE**
> Metric measurement alerts are currently in public preview.

ELEMENT NAME	REQUIRED	DESCRIPTION
TriggerCondition	Yes	Specifies whether the threshold is for total number of breaches or consecutive breaches from the following values: **Total** **Consecutive**
Operator	Yes	Operator for the comparison from the following values: **gt = greater than** **lt = less than**
Value	Yes	Number of the times the criteria must be met to trigger the alert.

Throttling

This section is optional. Include this section if you want to suppress alerts from the same rule for some amount of time after an alert is created.

ELEMENT NAME	REQUIRED	DESCRIPTION
DurationInMinutes	Yes if Throttling element included	Number of minutes to suppress alerts after one from the same alert rule is created.

EmailNotification

This section is optional Include it if you want the alert to send mail to one or more recipients.

ELEMENT NAME	REQUIRED	DESCRIPTION

ELEMENT NAME	REQUIRED	DESCRIPTION
Recipients	Yes	Comma delimited list of email addresses to send notification when an alert is created such as in the following example. **["recipient1@contoso.com", "recipient2@contoso.com"]**
Subject	Yes	Subject line of the mail.
Attachment	No	Attachments are not currently supported. If this element is included, it should be **None**.

Remediation

This section is optional Include it if you want a runbook to start in response to the alert. |

ELEMENT NAME	REQUIRED	DESCRIPTION
RunbookName	Yes	Name of the runbook to start.
WebhookUri	Yes	Uri of the webhook for the runbook.
Expiry	No	Date and time that the remediation expires.

Webhook actions

Webhook actions start a process by calling a URL and optionally providing a payload to be sent. They are similar to Remediation actions except they are meant for webhooks that may invoke processes other than Azure Automation runbooks. They also provide the additional option of providing a payload to be delivered to the remote process.

If your alert will call a webhook, then it will need an action resource with a type of **Webhook** in addition to the **Alert** action resource.

```
{
    "name": "<name-of-the-action>",
    "type": "Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions",
    "apiVersion": "<api-version-of-resource>",
    "dependsOn": [
        <name-of-schedule>
        <name-of-alert-action>
    ],
    "properties": {
        "etag": "*",
        "type": "Webhook",
        "name": "<display-name-of-action>",
        "severity": "<severity-of-alert>",
        "customPayload": "<payload-to-send>"
    }
}
```

The properties for Webhook action resources are described in the following tables.

ELEMENT NAME	REQUIRED	DESCRIPTION

ELEMENT NAME	REQUIRED	DESCRIPTION
type	Yes	Type of the action. This will be **Webhook** for webhook actions.
name	Yes	Display name for the action. This is not displayed in the console.
wehookUri	Yes	Uri for the webhook.
customPayload	No	Custom payload to be sent to the webhook. The format will depend on what the webhook is expecting.

Sample

Following is a sample of a solution that include that includes the following resources:

- Saved search
- Schedule
- Alert action
- Webhook action

The sample uses standard solution parameters variables that would commonly be used in a solution as opposed to hardcoding values in the resource definitions.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0",
    "parameters": {
      "workspaceName": {
        "type": "string",
        "metadata": {
          "Description": "Name of Log Analytics workspace"
        }
      },
      "accountName": {
        "type": "string",
        "metadata": {
          "Description": "Name of Automation account"
        }
      },
      "workspaceregionId": {
        "type": "string",
        "metadata": {
          "Description": "Region of Log Analytics workspace"
        }
      },
      "regionId": {
        "type": "string",
        "metadata": {
          "Description": "Region of Automation account"
        }
      },
      "pricingTier": {
        "type": "string",
        "metadata": {
          "Description": "Pricing tier of both Log Analytics workspace and Azure Automation account"
        }
      },
      "recipients": {
```

```
        "type": "string",
        "metadata": {
          "Description": "List of recipients for the email alert separated by semicolon"
        }
      }
    },
    "variables": {
      "SolutionName": "MySolution",
      "SolutionVersion": "1.0",
      "SolutionPublisher": "Contoso",
      "ProductName": "SampleSolution",

      "LogAnalyticsApiVersion": "2015-11-01-preview",

      "MySearch": {
        "displayName": "Error records by hour",
        "query": "Type=MyRecord_CL | measure avg(Rating_d) by Instance_s interval 60minutes",
        "category": "Samples",
        "name": "Samples-Count of data"
      },
      "MyAlert": {
        "Name": "[toLower(concat('myalert-',uniqueString(resourceGroup().id, deployment().name)))]",
        "DisplayName": "My alert rule",
        "Description": "Sample alert.  Fires when 3 error records found over hour interval.",
        "Severity": "Critical",
        "ThresholdOperator": "gt",
        "ThresholdValue": 3,
        "Schedule": {
          "Name": "[toLower(concat('myschedule-',uniqueString(resourceGroup().id, deployment().name)))]",
          "Interval": 15,
          "TimeSpan": 60
        },
        "MetricsTrigger": {
          "TriggerCondition": "Consecutive",
          "Operator": "gt",
          "Value": 3
        },
        "ThrottleMinutes": 60,
        "Notification": {
          "Recipients": [
            "[parameters('recipients')]"
          ],
          "Subject": "Sample alert"
        },
        "Remediation": {
          "RunbookName": "MyRemediationRunbook",
          "WebhookUri": "https://s1events.azure-automation.net/webhooks?
token=TluBFH3GpX4IEAnFoImoAWLTULkjD%2bTS0yscyrr7ogw%3d"
        },
        "Webhook": {
          "Name": "MyWebhook",
          "Uri": "https://MyService.com/webhook",
          "Payload": "{\"field1\":\"value1\",\"field2\":\"value2\"}"
        }
      }
    },
    "resources": [
      {
        "name": "[concat(variables('SolutionName'), '[' ,parameters('workspacename'), ']')]",
        "location": "[parameters('workspaceRegionId')]",
        "tags": { },
        "type": "Microsoft.OperationsManagement/solutions",
        "apiVersion": "[variables('LogAnalyticsApiVersion')]",
        "dependsOn": [
          "[resourceId('Microsoft.OperationalInsights/workspaces/savedSearches', parameters('workspacename'),
variables('MySearch').Name)]",
          "[resourceId('Microsoft.OperationalInsights/workspaces/savedSearches/schedules',
parameters('workspacename'), variables('MySearch').Name, variables('MyAlert').Schedule.Name)]",
          "[resourceId('Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions',
```

```
parameters('workspacename'), variables('MySearch').Name, variables('MyAlert').Schedule.Name,
variables('MyAlert').Name)]",
          "[resourceId('Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions',
parameters('workspacename'), variables('MySearch').Name, variables('MyAlert').Schedule.Name,
variables('MyAlert').Webhook.Name)]"
        ],
        "properties": {
          "workspaceResourceId": "[resourceId('Microsoft.OperationalInsights/workspaces',
parameters('workspacename'))]",
          "referencedResources": [
          ],
          "containedResources": [
            "[resourceId('Microsoft.OperationalInsights/workspaces/savedSearches',
parameters('workspacename'), variables('MySearch').Name)]",
            "[resourceId('Microsoft.OperationalInsights/workspaces/savedSearches/schedules',
parameters('workspacename'), variables('MySearch').Name, variables('MyAlert').Schedule.Name)]",
            "[resourceId('Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions',
parameters('workspacename'), variables('MySearch').Name, variables('MyAlert').Schedule.Name,
variables('MyAlert').Name)]",
            "[resourceId('Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions',
parameters('workspacename'), variables('MySearch').Name, variables('MyAlert').Schedule.Name,
variables('MyAlert').Webhook.Name)]"
          ]
        },
        "plan": {
          "name": "[concat(variables('SolutionName'), '[' ,parameters('workspaceName'), ']')]",
          "Version": "[variables('SolutionVersion')]",
          "product": "[variables('ProductName')]",
          "publisher": "[variables('SolutionPublisher')]",
          "promotionCode": ""
        }
      },
      {
        "name": "[concat(parameters('workspaceName'), '/', variables('MySearch').Name)]",
        "type": "Microsoft.OperationalInsights/workspaces/savedSearches",
        "apiVersion": "[variables('LogAnalyticsApiVersion')]",
        "dependsOn": [ ],
        "tags": { },
        "properties": {
          "etag": "*",
          "query": "[variables('MySearch').query]",
          "displayName": "[variables('MySearch').displayName]",
          "category": "[variables('MySearch').category]"
        }
      },
      {
        "name": "[concat(parameters('workspaceName'), '/', variables('MySearch').Name, '/',
variables('MyAlert').Schedule.Name)]",
        "type": "Microsoft.OperationalInsights/workspaces/savedSearches/schedules/",
        "apiVersion": "[variables('LogAnalyticsApiVersion')]",
        "dependsOn": [
          "[concat('Microsoft.OperationalInsights/workspaces/', parameters('workspaceName'),
'/savedSearches/', variables('MySearch').Name)]"
        ],
        "properties": {
          "etag": "*",
          "interval": "[variables('MyAlert').Schedule.Interval]",
          "queryTimeSpan": "[variables('MyAlert').Schedule.TimeSpan]",
          "enabled": true
        }
      },
      {
        "name": "[concat(parameters('workspaceName'), '/', variables('MySearch').Name, '/',
variables('MyAlert').Schedule.Name, '/',  variables('MyAlert').Name)]",
        "type": "Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions",
        "apiVersion": "[variables('LogAnalyticsApiVersion')]",
        "dependsOn": [
          "[concat('Microsoft.OperationalInsights/workspaces/', parameters('workspaceName'),
'/savedSearches/',  variables('MySearch').Name, '/schedules/', variables('MyAlert').Schedule.Name)]"
```

```
        ],
        "properties": {
          "etag": "*",
          "Type": "Alert",
          "Name": "[variables('MyAlert').DisplayName]",
          "Description": "[variables('MyAlert').Description]",
          "Severity": "[variables('MyAlert').Severity]",
          "Threshold": {
            "Operator": "[variables('MyAlert').ThresholdOperator]",
            "Value": "[variables('MyAlert').ThresholdValue]",
            "MetricsTrigger": {
              "TriggerCondition": "[variables('MyAlert').MetricsTrigger.TriggerCondition]",
              "Operator": "[variables('MyAlert').MetricsTrigger.Operator]",
              "Value": "[variables('MyAlert').MetricsTrigger.Value]"
            }
          },
          "Throttling": {
            "DurationInMinutes": "[variables('MyAlert').ThrottleMinutes]"
          },
          "EmailNotification": {
            "Recipients": "[variables('MyAlert').Notification.Recipients]",
            "Subject": "[variables('MyAlert').Notification.Subject]",
            "Attachment": "None"
          },
          "Remediation": {
            "RunbookName": "[variables('MyAlert').Remediation.RunbookName]",
            "WebhookUri": "[variables('MyAlert').Remediation.WebhookUri]"
          }
        }
      },
      {
        "name": "[concat(parameters('workspaceName'), '/', variables('MySearch').Name, '/',
variables('MyAlert').Schedule.Name, '/', variables('MyAlert').Webhook.Name)]",
        "type": "Microsoft.OperationalInsights/workspaces/savedSearches/schedules/actions",
        "apiVersion": "[variables('LogAnalyticsApiVersion')]",
        "dependsOn": [
          "[concat('Microsoft.OperationalInsights/workspaces/', parameters('workspaceName'),
'/savedSearches/', variables('MySearch').Name, '/schedules/', variables('MyAlert').Schedule.Name)]",
          "[concat('Microsoft.OperationalInsights/workspaces/', parameters('workspaceName'),
'/savedSearches/', variables('MySearch').Name, '/schedules/', variables('MyAlert').Schedule.Name,
'/actions/',variables('MyAlert').Name)]"
        ],
        "properties": {
          "etag": "*",
          "Type": "Webhook",
          "Name": "[variables('MyAlert').Webhook.Name]",
          "WebhookUri": "[variables('MyAlert').Webhook.Uri]",
          "CustomPayload": "[variables('MyAlert').Webhook.Payload]"
        }
      }
    ]
}
```

The following parameter file provides samples values for this solution.

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "workspacename": {
            "value": "myWorkspace"
        },
        "accountName": {
            "value": "myAccount"
        },
        "workspaceregionId": {
            "value": "East US"
        },
        "regionId": {
            "value": "East US 2"
        },
        "pricingTier": {
            "value": "Free"
        },
        "recipients": {
            "value": "recipient1@contoso.com;recipient2@contoso.com"
        }
    }
}
```

Next steps

- Add views to your management solution.
- Add Automation runbooks and other resources to your management solution.

Views in Operations Management Suite (OMS) management solutions (Preview)

4/12/2017 • 4 min to read • Edit Online

> **NOTE**
> This is preliminary documentation for creating management solutions in OMS which are currently in preview. Any schema described below is subject to change.

Management solutions in Operations Management Suite (OMS) will typically include one or more views to visualize data. This article describes how to export a view created by the View Designer and include it in a management solution.

> **NOTE**
> The samples in this article use parameters and variables that are either required or common to management solutions and described in Creating management solutions in Operations Management Suite (OMS)

Prerequisites

This article assumes that you're already familiar with how to create a management solution and the structure of a solution file.

Overview

To include a view in a management solution, you create a **resource** for it in the solution file. The JSON that describes the view's detailed configuration is typically complex though and not something that a typical solution author would be able to create manually. The most common method is to create the view using the View Designer, export it, and then add its detailed configuration to the solution.

The basic steps to add a view to a solution are as follows. Each step is described in further detail in the sections below.

1. Export the view to a file.
2. Create the view resource in the solution.
3. Add the view details.

Export the view to a file

Follow the instructions at Log Analytics View Designer to export a view to a file. The exported file will be in JSON format with the same elements as the solution file.

The **resources** element of the view file will have a resource with a type of **Microsoft.OperationalInsights/workspaces** that represents the OMS workspace. This element will have a subelement with a type of **views** that represents the view and contains its detailed configuration. You will copy the details of this element and then copy it into your solution.

Create the view resource in the solution

Add the following view resource to the **resources** element of your solution file. This uses variables that are described below that you must also add. Note that the **Dashboard** and **OverviewTile** properties are placeholders that you will overwrite with the corresponding properties from the exported view file.

```
{
    "apiVersion": "[variables('LogAnalyticsApiVersion')]",
    "name": "[concat(parameters('workspaceName'), '/', variables('ViewName'))]",
    "type": "Microsoft.OperationalInsights/workspaces/views",
    "location": "[parameters('workspaceregionId')]",
    "id": "[Concat('/subscriptions/', subscription().subscriptionId, '/resourceGroups/', resourceGroup().name,
'/providers/Microsoft.OperationalInsights/workspaces/', parameters('workspaceName'),'/views/',
variables('ViewName'))]",
    "dependson": [
        ],
    "properties": {
        "Id": "[variables('ViewName')]",
        "Name": "[variables('ViewName')]",
        "DisplayName": "[variables('ViewName')]",
        "Description": "",
        "Author": "[variables('ViewAuthor')]",
        "Source": "Local",
        "Dashboard": ,
        "OverviewTile":
    }
}
```

Add the following variables to the variables element of the solution file and replace the values to those for your solution.

```
"LogAnalyticsApiVersion": "2015-11-01-preview",
"ViewAuthor": "Your name."
"ViewDescription": "Optional description of the view."
"ViewName": "Provide a name for the view here."
```

Note that you could copy the entire view resource from your exported view file, but you would need to make the following changes for it to work in your solution.

- The **type** for the view resource needs to be changed from **views** to **Microsoft.OperationalInsights/workspaces**.
- The **name** property for the view resource needs to be changed to include the workspace name.
- The dependency on the workspace needs to be removed since the workspace resource isn't defined in the solution.
- **DisplayName** property needs to be added to the view. The **Id**, **Name**, and **DisplayName** must all match.
- Parameter names must be changed to match the required set of parameters.
- Variables should be defined in the solution and used in the appropriate properties.

Add the view details

The view resource in the exported view file will contain two elements in the **properties** element named **Dashboard** and **OverviewTile** which contain the detailed configuration of the view. Copy these two elements and their contents into the **properties** element of the view resource in your solution file.

Example

For example, the following sample shows a simple solution file with a view. Ellipses (...) are shown for the **Dashboard** and **OverviewTile** contents for space reasons.

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "workspaceName": {
            "type": "string"
        },
        "accountName": {
            "type": "string"
        },
        "workspaceRegionId": {
            "type": "string"
        },
        "regionId": {
            "type": "string"
        },
        "pricingTier": {
            "type": "string"
        }
    },
    "variables": {
        "SolutionVersion": "1.1",
        "SolutionPublisher": "Contoso",
        "SolutionName": "Contoso Solution",
        "LogAnalyticsApiVersion": "2015-11-01-preview",
        "ViewAuthor":  "user@contoso.com",
        "ViewDescription":  "This is a sample view.",
        "ViewName":  "Contoso View"
    },
    "resources": [
        {
            "name": "[concat(variables('SolutionName'), '(' ,parameters('workspacename'), ')')]",
            "location": "[parameters('workspaceRegionId')]",
            "tags": { },
            "type": "Microsoft.OperationsManagement/solutions",
            "apiVersion": "[variables('LogAnalyticsApiVersion')]",
            "dependsOn": [
                "[concat('Microsoft.OperationalInsights/workspaces/', parameters('workspacename'), '/views/',
variables('ViewName'))]"
            ],
            "properties": {
                "workspaceResourceId": "[concat(resourceGroup().id,
'/providers/Microsoft.OperationalInsights/workspaces/', parameters('workspacename'))]",
                "referencedResources": [
                ],
                "containedResources": [
                    "[concat('Microsoft.OperationalInsights/workspaces/', parameters('workspaceName'),
'/views/', variables('ViewName'))]"
                ]
            },
            "plan": {
                "name": "[concat(variables('SolutionName'), '(' ,parameters('workspaceName'), ')')]",
                "Version": "[variables('SolutionVersion')]",
                "product": "ContosoSolution",
                "publisher": "[variables('SolutionPublisher')]",
                "promotionCode": ""
            }
        },
        {
            "apiVersion": "[variables('LogAnalyticsApiVersion')]",
            "name": "[concat(parameters('workspaceName'), '/', variables('ViewName'))]",
            "type": "Microsoft.OperationalInsights/workspaces/views",
            "location": "[parameters('workspaceregionId')]",
            "id": "[Concat('/subscriptions/', subscription().subscriptionId, '/resourceGroups/',
resourceGroup().name, '/providers/Microsoft.OperationalInsights/workspaces/',
parameters('workspaceName'),'/views/', variables('ViewName'))]",
            "dependson": [
            ],
            "properties": {
```

```
                "Id": "[variables('ViewName')]",
                "Name": "[variables('ViewName')]",
                "DisplayName": "[variables('ViewName')]",
                "Description": "[variables('ViewDescription')]",
                "Author": "[variables('ViewAuthor')]",
                "Source": "Local",
                "Dashboard": ...,
                "OverviewTile": ...
            }
        }
      ]
}
```

Next steps

- Learn complete details of creating management solutions.
- Include Automation runbooks in your management solution.

Best practices for creating management solutions in Operations Management Suite (OMS) (Preview)

4/27/2017 • 2 min to read • Edit Online

> **NOTE**
> This is preliminary documentation for creating management solutions in OMS which are currently in preview. Any schema described below is subject to change.

This article provides best practices for creating a management solution file in Operations Management Suite (OMS). This information will be updated as additional best practices are identified.

Data sources

- Data sources can be configured with a Resource Manager template, but they should not be included in a solution file. The reason is that configuring data sources is not currently idempotent meaning that your solution could overwrite existing configuration in the user's workspace.

  For example, your solution may require Warning and Error events from the Application event log. If you specify this as a data source in your solution, you risk removing Information events if the user had this configured in their workspace. If you included all events, then you may be collecting excessive Information events in the user's workspace.

- If your solution requires data from one of the standard data sources, then you should define this as a prerequisite. State in documentation that the customer must configure the data source on their own.

- Add a Data Flow Verification message to any views in your solution to instruct the user on data sources that need to be configured for required data to be collected. This message is displayed on the tile of the view when required data is not found.

Runbooks

- Add an Automation schedule for each runbook in your solution that needs to run on a schedule.
- Include the IngestionAPI module in your solution to be used by runbooks writing data to the Log Analytics repository. Configure the solution to reference this resource so that it remains if the solution is removed. This allows multiple solutions to share the module.
- Use Automation variables to provide values to the solution that users may want to change later. Even if the solution is configured to contain the variable, it's value can still be changed.

Views

- All solutions should include a single view that is displayed in the user's portal. The view can contain multiple visualization parts to illustrate different sets of data.
- Add a Data Flow Verification message to any views in your solution to instruct the user on data sources that need to be configured for required data to be collected.
- Configure the solution to contain the view so that it's removed if the solution is removed.

Alerts

- Define the recipients list as a parameter in the solution file so the user can define them when they install the solution.
- Configure the solution to reference alert rules so that user's can change their configuration. They may want to make changes such as modifying the recipient list, changing the threshold of the alert, or disabling the alert rule.

Next steps

- Walk through the basic process of designing and building a management solution.
- Learn how to create a solution file.
- Add saved searches and alerts to your management solution.
- Add views to your management solution.
- Add Automation runbooks and other resources to your management solution.

Integrating with Operations Management Suite (OMS)

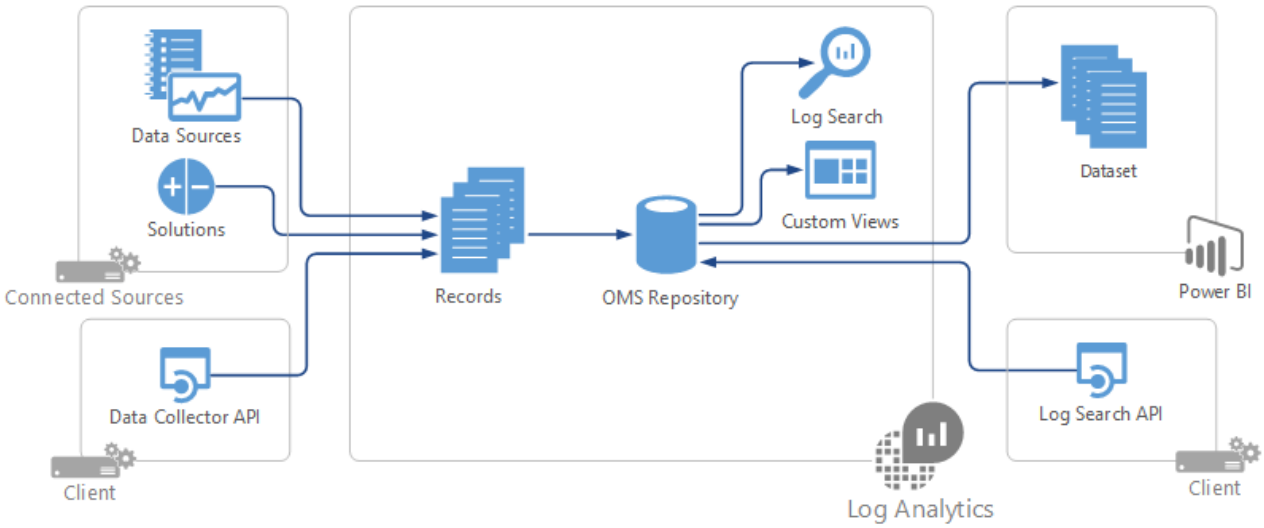
4/12/2017 • 5 min to read • Edit Online

Operations Management Suite is Microsoft's cloud-based IT management solution that helps you manage and protect your on-premises and cloud infrastructure. In addition to using the standard features of OMS, you can integrate it with other management applications and services to provide a hybrid management environment, to provide custom management scenarios unique to your environment, or to provide a custom management experience for your customers. This article provides an overview of your different options for integrating with OMS services and links to articles providing detailed technical information.

Log Analytics

Management data collected by Log Analytics is stored in a repository which is hosted in Azure. All data stored in the repository is available in log searches which provide quick analysis across extremely large amounts of data. Your integration requirements may be to populate the repository with new data making it available for analysis, or to extract data in the repository to provide a new visualization or to integrate with another management tool.

Each piece of data in the repository is stored as a record. When you populate the repository, you should provide users with the record type that your solution uses and a description of its properties. When you retrieve data, you need this information about the data you're working with.



Populate the Log Analytics repository

There are multiple methods for populating the OMS repository. The method that you use will depend on factors such as where the source data is located, the format of the data, and which clients you need to support. Once data is stored in the repository, it makes no difference how it was collected.

The following sections describe the different options for populating the OMS repository.

Connected Sources and Data sources

Connected sources are the locations where data can be retrieved for the OMS repository. Data Sources and Solutions run on Connected Sources and define the specific data that's collected. If your application writes data to one of these data sources, then you can collect it by configuring the data source. For example, if your application creates Syslog events, then they can be collected by the Syslog data source on a Linux agent.

- Data sources in Log Analytics

Solutions

Solutions extend the capabilities of OMS. A solution may collect data from the connected source or it may perform analysis on records already collected in the repository. Each solution provided by Microsoft has an individual article that provides the details on the data that it collects.

- Solutions in Log Analytics

HTTP Data Collector API

The Log Analytics HTTP Data Collector API is a REST API that allows you to add JSON data to the Log Analytics repository. You can leverage this API when you have an application that doesn't provide data through one of the other data sources or solutions. It can be used to populate the repository from any client that can call the API and does not rely on the collection schedule of any data source or solution.

- Log Analytics HTTP Data Collector API

Retrieve data from the Log Analytics repository

There are multiple methods for retrieving data from the OMS repository. You may want users to retrieve data using the OMS console and provide them with different kinds of visualizations and analysis. You can also retrieve the data from an external process such as another management solution.

Log searches

All data stored in the OMS repository is available through log searches. Users may perform their own ad hoc analysis in the OMS console or create a dashboard with a visualization for a particular log search. Solutions can contain custom views with visualizations based on predefined searches. You can use the Log Search API to access data in the OMS repository from an external application or management tool.

- Log searches in Log Analytics
- Log Analytics log search REST API
- Log Analytics cmdlets

Custom views

The View Designer allows you to create custom views in the OMS console that provide users with visualization and analysis of the data in your solution. Each view includes a tile that's displayed on the main page of the console and any number of visualization parts that are based on log searches that you define.

- Log Analytics View Designer

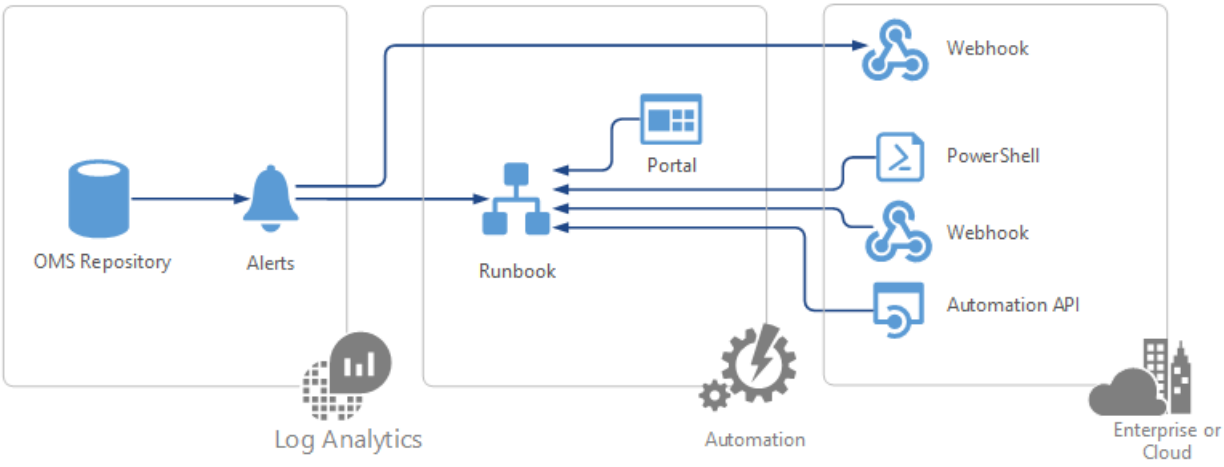
Power BI

Log Analytics can automatically export data from the OMS repository into Power BI so you can leverage its visualizations and analysis tools. It performs this export on a schedule so the data is kept up to date.

- Export Log Analytics data to Power BI

Automation

OMS can automate processes to react to collected data or to perform other management functions. It may collect data from your application and insert it into the OMS repository, or you may automate the correction of a known issue in response to data found in the repository.



Runbooks

Runbooks in Azure Automation run PowerShell scripts and workflows in the Azure cloud. You can use them to manage resources in Azure or any other resources that can be accessed from the cloud. Runbooks can also be run in a local datacenter using Hybrid Runbook Worker. You can start a runbook from the Azure portal or from external processes using a number of methods such as PowerShell or the Automation API.

- Starting a runbook in Azure Automation
- Azure Automation cmdlets
- Automation REST API
- Automation .NET

Alerts

Alert rules automatically run log searches according to a schedule. If the results match particular criteria the resulting alert can start a runbook in Azure Automation or call a webhook which can start an external process. Both of these responses can include details of the alert including the data returned in the log search.

- Alerts in Log Analytics
- Log Analytics Alert API

Backup and Site Recovery

Azure Backup and Site Recovery provide services for protecting your enterprise data and ensuring the availability of servers and applications. You can leverage these services to perform such scenarios as providing backup services for your application or initiating a failover of a virtual machine.

- Azure Backup cmdlets
- Azure Site Recovery REST API
- Azure Site Recovery Cmdlets

Custom solutions

You can encapsulate integration logic into a custom solution to run in your workspace or in a customer's workspace. Your solution can include any of the integration methods in this article in addition to other resources to provide a complete management scenario. The resources in the solution are packaged such that when the solution is removed, all of the resources that it created are removed from the OMS workspace and Azure subscription.

For example, your solution could include an Automation runbook to gather and process data and then populate the Log Analytics repository using the HTTP Data Collector API. You could also include a custom view that presents and analyzes the collected data.

- Creating custom solutions (Coming soon)

Next steps

- Reference the OMS SDK for technical information on automating OMS services.

Operations Management Suite (OMS) SDK

3/2/2017 • 1 min to read • Edit Online

Operations Management Suite (OMS) is Microsoft's cloud-based IT management solution that helps you manage and protect your on-premises and cloud infrastructure. This article lists the documentation and other resources available for accessing OMS services outside of the OMS and Azure portals. This includes REST API for access from various programming interfaces and scripting engines such as PowerShell.

Automation

- Azure Automation documentation
- Automation PowerShell Cmdlets
- Automation REST API
- Community runbooks

Backup

- Azure Backup documentation
- Backup PowerShell Cmdlets
- Backup REST API
- Deploy and manage backup to Azure for Windows Server/Windows Client using PowerShell

Log Analytics

- Log Analytics documentation
- Log Analytics REST API
- Log Analytics HTTP Data Collector API
- Log Search REST API
- Alert REST API
- Log Analytics PowerShell Cmdlets
- Log Analytics .NET Library

Service Map

- Service Map documentation
- Service Map REST API

Site Recovery

- Site Recovery PowerShell cmdlets
- Site Recovery REST API
- Add Azure Automation runbooks to recovery plans
- Replicate between on-premises Hyper-V virtual machines and Azure by using PowerShell and Azure Resource Manager

Next steps

- Read about the different options for integrating with OMS services.

- Create a custom solution in OMS.