

EVIDEN LANDING ZONES FOR AZURE VM OS MANAGEMENT REPORTING DASHBOARD AND WORKBOOK INSTRUCTION MANUAL

Author(s)	:	Klaas Jan de Jager
Version	:	1.0
Status	:	Final
Source	:	Eviden Landing Zones for Azure
Document date	:	8 April 2024
Number of pages	:	39

Contents

List of changes	3
1. Eviden Landing Zones for Azure VM OS Management Reporting Dashboard	4
2. Backup Center	7
3. Backup workbook	9
3.1 VM backup configuration.....	9
3.2 Retention period per Backup Policy	10
3.3 Backup jobs status for VMs.....	10
3.4 Overall Backup Status overview	11
3.5 Distribution of Jobs in Period by Backup Item overview	13
3.6 List of Jobs in Period	13
4. Availability workbook.....	15
5. Performance workbook	17
6. Security Posture.....	22
7. VM OS Image gallery workbook	23
8. VM Tagging workbook.....	25
9. Antimalware workbook.....	26
10. Availability Sets workbook	28
10.1 Overview availability sets	28
10.2 Overview virtual machines in availability sets.....	29
11. Scale Sets workbook	30
11.1 Overview scale sets	30
11.2 Scale Set Details	32
12. Disk Encryption workbook	33
13. Storage Accounts workbook	35
13.1 Storage account Configuration Overview	35
13.2 Storage Accounts Workloads	35
13.3 Storage Accounts Workloads Overview blade	36
13.4 Storage Accounts Workloads Capacity blade	37
13.5 Storage Accounts Workloads Usage blade.....	38

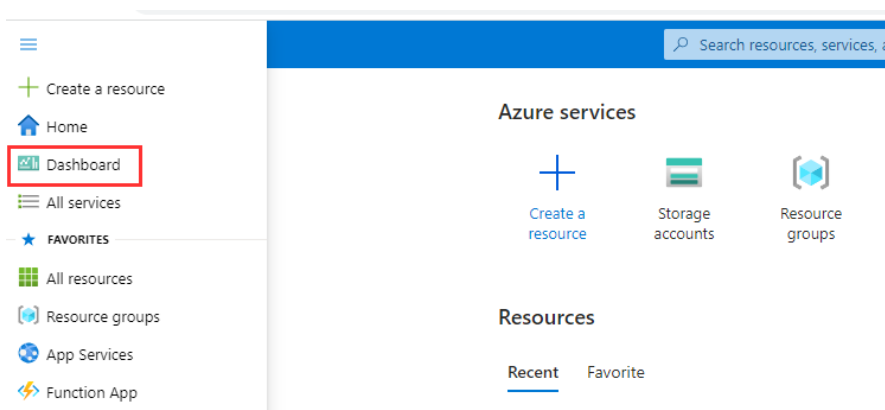
List of changes

Version	Date	Description	Author(s)
1.0	22-08-2023	Initial Eviden version	K.J. de Jager

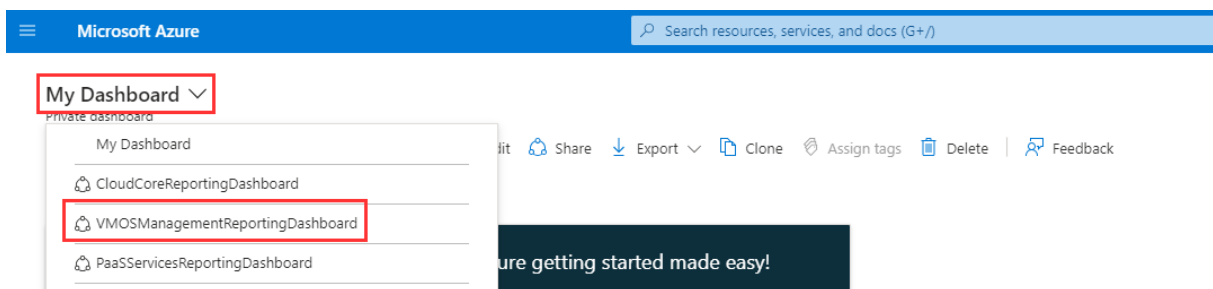
1. Eviden Landing Zones for Azure VM OS Management Reporting Dashboard

This dashboard is an entry point that guides you to get most of the insights of your cloud environment. The dashboard consists of several tiles that direct you to the concerning Azure blade or workbook. You can scroll up and down through the dashboard to see all tiles. In the following paragraphs all tiles and workbooks will be shortly described.

To access the shared dashboard simply click on the menu on the top left in the portal. By default, "Dashboard" button is set on the top, see image below.



This should directly send you to the correct dashboard. If this is not the case, change the dashboard add the left top corner by clicking on the dashboard title and select VMOSManagementReportingDashboard, see image below.



Note: In case the environment has been upgraded from a previous release, it is possible that 'old dashboard names' may still appear in this overview. Once one of these is selected, an error message should be shown, and after that, the dashboard will disappear from the dropdown menu.

The VM OS Management Reporting dashboard, as in the next picture, now appears:

VMOSManagementReportingDash...
Shared dashboard

+ Create ↑ Upload ↺ Refresh ✓ Full screen | Edit Manage sharing ↓ Export ↵ Clone Assign tags Delete | Feedback

Auto refresh: Off UTC Time: Past 24 hours Add filter

Getting Started with VM OS Reporting

First time using this dashboard?
Left: Instruction Manual
Right: VM Tagging Manual

EVIDEN

Eviden Landing Zones for Azure - VM OS Management Reporting dashboard

Deploy VM
Deploy Virtual Machine to be Eviden Managed

UI VM templates

Available Virtual Machines
Private Resource Graph query

Download formatted results as CSV

Formatted results On

Name	Location	Resource group	Subscription	OSType	SKU	VMSize	diskEncryptionState
alkeshvmfordevelop	UK South	alkeshvmfordevelop	UK South	Windows	win11-22h2-pro	Standard_B2ms	SSE with PMK
snowpocfred001	UK South	snowpocfred001	UK South	Linux	11-gen2	Standard_D4s_v3	SSE with PMK
linvm03	UK South	linvm03	UK South	Linux	87-gen2	Standard_DS1_v2	SSE with PMK
wimvm08	UK South	wimvm08	UK South	Windows	2016-datacenter-gens...	Standard_DS1_v2	SSE with PMK
wimvm07	UK South	wimvm07	UK South	Windows	2016-datacenter-gens...	Standard_DS1_v2	SSE with PMK
linvm01	UK South	linvm01	UK South	Linux	20_04-lts-gen2	Standard_DS1_v2	SSE with PMK
linvm02	UK South	linvm02	UK South	Linux	gen2	Standard_DS1_v2	SSE with PMK

Backup/Restore documentation

Left: Self Service Restore
Right: How to take app-consistent backup (Linux)

Backup Center
Azure Monitor

Availability
Azure Monitor

Performance
Azure Monitor

Security Posture
Azure Monitor

VM OS Image Gallery
Azure Monitor

Backup
Azure Monitor

VM Tagging
Azure Monitor

Antimalware
Azure Monitor

Availability Sets
Azure Monitor

The tile **“Getting Started with VM OS Management Reporting” [1]** contains 2 icons:

- The left-hand icon redirects you to the up-to-date version of the Getting Started manual (this document).
- The right-hand icon redirects to the VM Tagging Manual that contains an overview of the Eviden managed tags that can be used to enable certain VM management or monitoring features.

Below the Getting Started tile you will find an overview with **Available Virtual machines [2]**. In this overview you will find all deployed virtual machines in the environment together with the configuration information for the VM, like:

- Location

- Resource group
- Subscription
- OSType
- SKU
- VMSize
- diskencryptionState

By selecting the **VM Name [3]** in this overview you will be redirected to the VM blade in Azure.

The overview also provides the option **"Download formatted result as CSV" [4]** to export the overview as a CSV file and import this file in Excel.

The **"Backup/Restore documentation" [5]** is an informational tile that redirects to Microsoft Azure documentation pages.

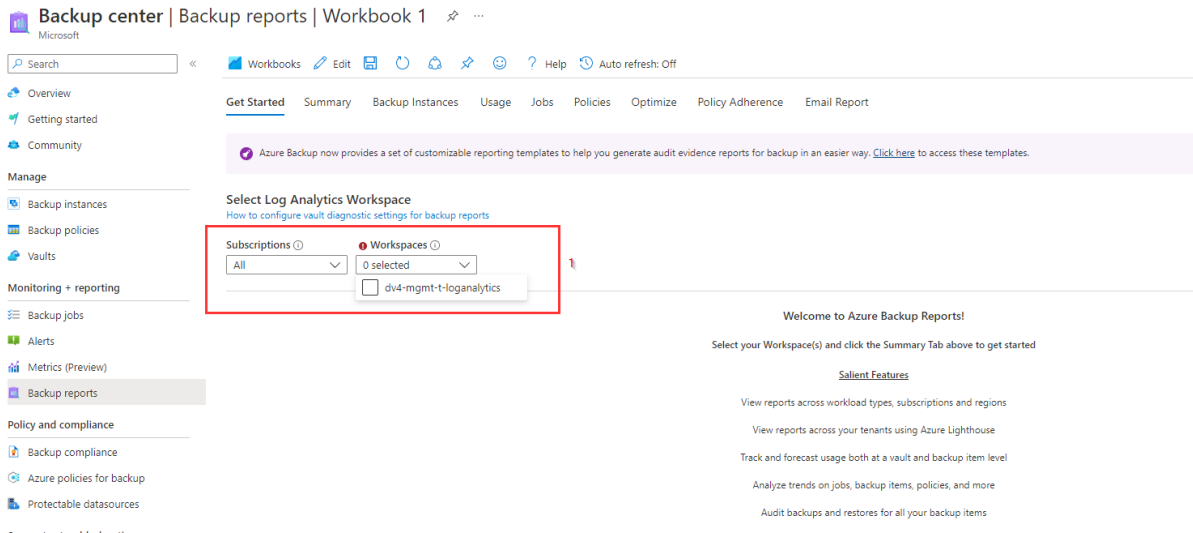
- The left-hand icon redirects to [Self Service restore](#) documentation.
- The right-hand icon redirects to documentation about [App-consistent backups of Linux VMs](#).

The **"Deploy VM" tile [6]** includes two links that customers can use to quickly deploy a managed VM with VM tags and tag values set. Two icons are displayed, each of them will open a new browser tab:

- **UI definition** Azure UI Definition, which offers a streamlined interface within the Azure Portal to deploy supported Windows or Linux VMs with the correct set of tags. End users just need to review and/or change the parameters and then create the VM.
- **VM templates** Redirects to the repository with ARM templates for all currently supported OS types. The templates already have VM tags and tag values correctly set. The templates can be used to deploy Eviden Managed VMs programmatically (through API, CICD pipeline, etc).

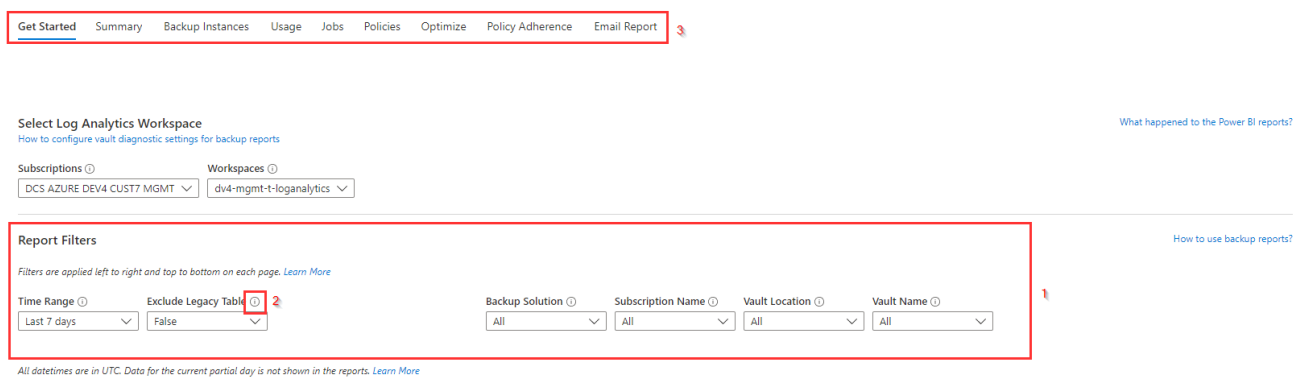
2. Backup Center

The Backup Center tile directs you to the Azure Backup Center Blade.



This is a backup reporting blade provided from Azure it selves to provide several backup reports. When this blade is opened you enter the first tab (**Getting Started**) [2] where you first need to select the **Eviden managed** log analytics workspace that is in the management subscription. In Eviden Landing Zones for Azure there is by default only one **log analytics workspace** [1] available in the management subscription. If you see more then one log analytics workspace in the management subscription, you need to find the log analytics workspace that hat the *tag EvidenPurpose = EvidenMonitoring* and select this one.

After you selected the log analytics workspace in the Getting Started tab, you find several additional **report filters** [1] in this tab to set the required **Time Range, Exclude Legacy Table, Backup Solution, Subscription Name, Vault Location** and **Vault Name**.



8 April 2024

For internal use

Version: 1.0

These filters can be used to select which backups will be reported on and in what time window. For more information about a specific filter you can use the **information sign [2]** at the right site of each filter name.

If all filters are set as required you can select one of the other **tabs at the top [3]** to view some specific reports about the backups for selected filters.

As these backup reports are a default feature of Microsoft Azure there will be no extensive description of each tab here but instead a link to the Microsoft description of each tab is provided below:

- **Summary:** Use this tab to get a high-level overview of your backup estate. [Learn more](#)
- **Backup Instances:** Use this tab to see information and trends on cloud storage consumed at backup-item level. [Learn more](#)
- **Usage:** Use this tab to view key billing parameters for your backups. [Learn more](#)
- **Jobs:** Use this tab to view long-running trends on jobs, such as number of failed jobs per day and the top causes of job failure. [Learn more](#)
- **Policies:** Use this tab to view information on all your active policies, such as the number of associated items and the total storage consumed by items backup up under a given policy. [Learn more](#)
- **Optimize:** Use this tab to gain visibility into potential cost-optimization opportunities for your backup. [Learn more](#)
- **Policy adherence:** Use this tab to gain visibility into whether every backup instance has had at least one successful backup per day. [Learn more](#)

Email Report: Using the Email Report feature available in Backup Reports, you can create automated tasks to receive periodic reports via email. This feature works by deploying a logic app in your Azure environment that queries data from your selected Log Analytics (LA) workspaces, based on the inputs that you provide. [Learn more](#)

3. Backup workbook



The Backup workbook consist of 3 parts:






- VM backup configuration.
- Retention period per Backup Policy.
- Backup jobs status for VMs.





Each part of this report will be described in the next sections.

3.1 VM backup configuration

At the top of the report there are several filters to select on Subscription, VM Name, VM Backup State and Policies (EvidenBackup tag).

Backup  
Azure Monitor

Workbooks     ? Help  Auto refresh: Off

Subscription  VM Name  VM Backup State  Policies (EvidenBackup ...) 

1 2 3 4 5 6 7

VM backup configuration

VM Name	ResourceGroup	Subscription	VM Backup State	Policy (EvidenBackup tag)
winvm06	rsg-vms	LND1	VM is EvidenManaged, but not in Backup	-
winvms07	rsg-vms	LND1	VM does not have the correct tags	-
LINVMO1	rsg-vms	LND2	VM is EvidenManaged, but not in Backup	-
linvm02	rsg-vms	LND2	VM is EvidenManaged, but not in Backup	-
linvm03	rsg-vms	LND1	VM is EvidenManaged and in Backup	Gold
WINVM03	rsg-vms	LND2	VM is EvidenManaged and in Backup	Gold
winvm01	rsg-vms	LND1	VM does not have the correct tags	Silver

The **Subscription [1]** filter applies for both this part and the second part of the workbook. The other filters only applies to this part of the report.

The **VM Name [2]** filter can be used to filter on one or more specific VM's within the selected subscriptions. The **VM Backup State [3]** filter and the **Policies (EvidenBackup tag) [4]** filter can be used to filter on the **VM Backup State [5]** column and **Policy (EvidenBackup tag) [6]** column respectively.

This **VM backup configuration** overview provides insight in the backup configuration of all VMs, depending on the filters set, based on the settings for the **EvidenManaged** and **EvidenBackup** tag that are used to configure backups for the virtual machines within Eviden Landing Zones for Azure.

The **VM Backup State [5]** column shows, based on the tag values for **EvidenManaged** and **EvidenBackup**, if a VM is managed by Eviden and has a backup schedule defined. There are 3 possible VM states for backup:

- **VM does not have the correct tags:** In this state the **EvidenManaged** tag is **not set** (to "True") for the VM.

- **VM is EvidenManaged, but not in Backup:** This state means that the **EvidenManaged** tag is set to "True", but the **EvidenBackup** tag is not set or has an empty value.
- **VM is EvidensManaged and in Backup:** In this state the **EvidenManaged** tag is set to "True" and the **EvidenBackup** tag is set to a *backup policy*.

If a VM is EvidenManaged and in Backup, in the **Policy (EvidenBackup tag)** [6] column the backup policy that is set can be found.

At the right site of the overview the **Export [7]** button is available to export this overview as a CSV-file.

To check the settings for a specific VM it's possible to click on a **VM name [8]** in the VM Name column to be redirected to the VM configuration blade in Azure.

3.2 Retention period per Backup Policy

The second part of this report provides an overview of every defined backup policy with the backup frequencies and the backup retention period that are available within the selected subscriptions at the Subscription filter on top of this report.

At the top of this part there is a filter [1] to filter the Defined Policies by name.

Defined Policies									
All									
Retention period per Backup Policy									
BackupPolicy	Subscription	Frequency	RetentionDaily	RetentionWeekly	RetentionMonthly	RetentionYearly			
DefaultPolicy	LND1	Daily	Retain backup taken every day for 30 days						
DefaultPolicy	LND2	Daily	Retain backup taken every day for 30 days						
EnhancedPolicy	LND1	Hourly	Retain backup taken every day for 30 days						
EnhancedPolicy	LND2	Hourly	Retain backup taken every day for 30 days						
HourlyLogBackup	LND1								
HourlyLogBackup	LND2								
Bronze	LND2	Daily	Retain backup taken every day for 15 days	Retain backup taken every week for 8 weeks	Retain backup taken every month for 6 months				
Bronze	LND1	Daily	Retain backup taken every day for 15 days	Retain backup taken every week for 8 weeks	Retain backup taken every month for 6 months	Retain backup taken every year for 2 years			
Gold	LND1	Daily	Retain backup taken every day for 15 days	Retain backup taken every week for 8 weeks	Retain backup taken every month for 6 months	Retain backup taken every year for 2 years			
Gold	LND2	Daily	Retain backup taken every day for 15 days	Retain backup taken every week for 8 weeks	Retain backup taken every month for 6 months	Retain backup taken every year for 2 years			
Silver	LND2	Daily	Retain backup taken every day for 15 days	Retain backup taken every week for 8 weeks	Retain backup taken every month for 6 months	Retain backup taken every year for 2 years			

As the backup Policies are defined per subscription it's possible to have several backup policies with the same name as is visible in the **BackupPolicy [2]** column. In the **Frequency [3]** column the backup frequency for each policy is visible, while in the last 4 **columns [4]** the **daily**, **weekly**, **monthly** and **yearly** retention is shown, if applicable.

At the right site of the overview the **Export [5]** button is available to export this overview as a CSV-file.

3.3 Backup jobs status for VMs

This part consist of one Job reports blade to show the status information about the backup jobs based on the filters at the top of this blade.

Backup jobs status for VMs

Jobs Reports

Subscriptions

Workspaces

All

Any one

Report Filters

Time Range

Exclude Legacy Table

Last 3 days

False

Backup Solution

Subscription Name

Vault Location

Vault Name

All

All

All

All

All datetimes are in UTC. Data for the current partial day is not shown in the reports. [Learn More](#)

In this overview the **Eviden managed log analytics workspace** that is in the **management subscription** is selected by default based on the Subscription and Workspace [1] filter. There is no need to change the **Subscription** and **Workspace** filters as in Eviden Landing zones for Azure there is by default only one log analytics workspace available in the management subscription that has the tag *EvidenPurpose = EvidenMonitoring*, so "Any one" as is in the Workspaces filter should reflect to this Eviden Managed log analytics workspace.

In the **Report Filters** section there are 6 filters to filter a specific Time Range [2], between *Last 3 days* and *Last 90 days* or a *Custom* time range, and on specific backup jobs:

The **Exclude Legacy Table [3]** filter can be used to avoid querying data that is sent to the legacy Azure Diagnostics table. Excluding the legacy table improves query performance time.

Backup Solution [4] filter is used to filter on specific backup solutions, like *Azure backup Agent, Azure Backup Server, Azure Storage Backup, Azure Virtual Machine Backup, DPM, SAP HANA or SQL in Azure VM Backup*.

The **Subscription Name, Vault Location and Vault Name filters [5]** are used to filter on Vaults in a specific subscription, location or on a specific vault name.

When the log analytics workspace and the report filters are set, 3 backup report overviews are shown:

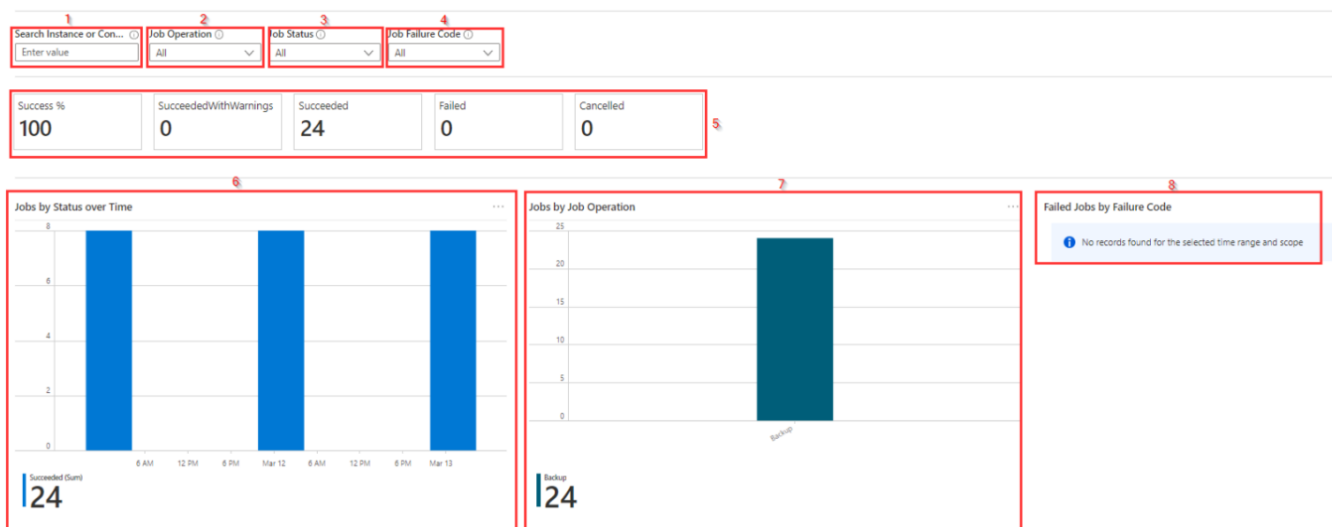
- An overall backup status overview with success rate and graphical status information.
- Distribution of Jobs in Period by Backup Item
- List of Jobs in Period

3.4 Overall Backup Status overview

The overall backup status overview by default shows the status of all backup jobs for VM (instances) within the report filters set.

At the top of this overview there are some additional filters to filter on specific backup jobs:

- **Search Instance or Container [1]:** Use to search for a backup instance by name.
To search for a specific instance in a container, use the syntax [container name];[instance name]
To search for all instances in a container, use the syntax [container name];
- **Job Operation [2]:** Use to filter by job operation like *Backup* or *Restore*
- **Job Status [3]:** Use to filter by job status like *Succeeded*, *Failed*, *SucceededWith Warnings* or *Cancelled*.
- **Job Failure Code [4]:** Use to filter by failure code if any jobs are failed.



In this report you first find an overview with the percentage success rate of the backup jobs within the selected time range and at the right side of this **Success %** the numbers of **SucceededWithWarnings**, **Succeeded**, **Failed** or **Canceled** are shown.

If in the **Search Instance or Container [1]** a specific instance or container is entered, the percentage and numbers for that instance or container is shown.

Below this overview a graphical overview is shown with **Jobs by Status over Time [6]**, **Jobs by Job Operation [7]** and **Failed Jobs by Failure Code [8]** (if any).

3.5 Distribution of Jobs in Period by Backup Item overview

Below the Overall Backup Status overview you find a more detailed overview about the backup jobs on a backup item bases. In this overview there are some drop down tiles [1] to be able to select the look and feel of the overview. These settings do not only impact the look and feel for the overview at the screen but also for the **export [2]** option at the right top of this overview.

Distribution of Jobs in Period by Backup Item

Sort By () Order () Rows per Page () Page ()

Avg data transferred (MB) Descending 10 1 of 2

Backup Instance	Container	Resource Group	# Jobs Failed	Job Success %	Avg Data Transferred (MB)	Avg Job Duration (hrs)	Azure Resource
linvm89	linvm89	Default (group1)	0	100.0 %	1,114.00	0.35	linvm89
winvm98	winvm98	Default (group1)	0	100.0 %	909.67	0.35	winvm98
winvm88	winvm88	Default (group1)	0	100.0 %	863.33	0.35	winvm88
linvm98	linvm98	Default (group1)	0	100.0 %	854.67	0.35	linvm98
winvm99	winvm99	Default (group1)	0	100.0 %	773.00	0.46	winvm99
winvm87	winvm87	Default (group1)	0	100.0 %	652.67	0.35	winvm87
winvm89	winvm89	Default (group1)	0	100.0 %	644.67	0.46	winvm89
linvm99	linvm99	Default (group1)	0	100.0 %	244.00	0.41	linvm99
dv4testvm1-win	Dv4TestVM1-Win	Default (group1)	0	-	-	-	DV4TESTVM1-WIN
dv4testvm1-lin	Dv4TestVM1-Lin	Default (group1)	0	-	-	-	DV4TESTVM1-LIN

Click on any row above to see details of all jobs for that backup item in the selected time range.

In the overview you can select a specific **backup instance [3]** in the Backup Instance column to be redirected to that specific backup item blade and get some more detailed information.

In the same way you can select a **Resource/VM name [4]** in the Azure Resource column to be redirected to the VM or Resource blade in Azure.

By selecting on any of the rows (not in the Backup Instance or Azure Resource column, as you will be redirected to the respective blades then) as mentioned in the **bottom text of this overview [5]** you will get a detailed list of jobs for that backup item for the selected Time Range.

3.6 List of Jobs in Period

This overview shows a list of jobs for the selected backup item in the above overview with some detailed information about each backup job.

Distribution of Jobs in Period by Backup Item

Sort By Order Rows per Page Page

Backup Instance	Container	Resource Group	# Jobs Failed	Job Success %	Avg Data Transferred (MB)	Avg Job Duration (hrs)	Azure Resource
winvm01	winvm01	winvm01-rg	0	100.0 %	1,114.00	0.35	WINVM01
winvm02	winvm02	winvm02-rg	0	100.0 %	809.87	0.35	WINVM02
winvm03	winvm03	winvm03-rg	0	100.0 %	853.33	0.35	WINVM03
winvm04	winvm04	winvm04-rg	0	100.0 %	854.87	0.35	WINVM04
winvm05	winvm05	winvm05-rg	0	100.0 %	773.00	0.46	WINVM05
winvm06	winvm06	winvm06-rg	0	100.0 %	652.87	0.35	WINVM06
winvm07	winvm07	winvm07-rg	0	100.0 %	644.87	0.46	WINVM07
winvm08	winvm08	winvm08-rg	0	100.0 %	244.00	0.41	WINVM08
winvm09	winvm09	winvm09-rg	0	100.0 %	244.00	0.41	WINVM09
winvm10	winvm10	winvm10-rg	0	100.0 %	244.00	0.41	WINVM10

Click on any row above to see details of all jobs for that backup item in the selected time range.

List of Jobs in Period

Sort By Order Rows per Page Page

Backup Instance	Container	Resource Group	Operation Category	Job Status	Job Start Date Time	Job Duration	Job Failure Code	Data Trans.	Azure Resource	Datasource Type
winvm01	winvm01	winvm01-rg	Backup	Completed	3/13/2023, 10:40:16 AM	0.35	Success	1779	WINVM01	Microsoft.Compute/VirtualMachines
winvm02	winvm02	winvm02-rg	Backup	Completed	3/12/2023, 10:31:30 AM	0.35	Success	0	WINVM02	Microsoft.Compute/VirtualMachines
winvm03	winvm03	winvm03-rg	Backup	Completed	3/11/2023, 10:35:11 AM	0.35	Success	800	WINVM03	Microsoft.Compute/VirtualMachines

The look and feel can be changed by using the **drop down tiles [1]** at the top of this overview and based on these settings the result can be **exported [2]** as a CSV. For the export option you need to click on **three-dots [3]** at the right top of the overview.

4. Availability workbook

The Availability report is used to provide an overview of the availability of VM's for a selected time range.

Dashboard > Availability Azure Monitor

Workbooks Edit Help Auto refresh Off

TimeRange: Last 12 hours Subscription: All Workspace: All Servers: All Managed by Eviden: All Powerstate: All

VM Availability Overview

Virtual Machine	Resource Group	Managed by Eviden	Powerstate	Monitoring Agent	Last HeartBeat within time range	Available Hours	Total Hours	Availability
lnvm03	dv4-Ind1-t-rsg-vms	Yes	VM running	Enabled for selected workspace	09/08/2023, 10:40:07	12	12	100%
lnvm01	dv4-Ind1-t-rsg-vms	No	VM running	Enabled for selected workspace	09/08/2023, 10:39:32	12	12	100%
lnvm06	dv4-Ind1-t-rsg-vms	Yes	VM running	Enabled for selected workspace	09/08/2023, 10:40:21	12	12	100%
lnvm07	dv4-Ind1-t-rsg-vms	No	VM running	Enabled for selected workspace	09/08/2023, 10:40:09	12	12	100%
UNVM01	dv4-Ind2-t-rsg-vms	Yes	VM running	Enabled for selected workspace	09/08/2023, 08:13:50	12	12	100%
UNVM01	dv4-Ind2-t-rsg-vms	Yes	VM running	Enabled for selected workspace	09/08/2023, 10:39:50	12	12	100%
lnvm02	dv4-Ind2-t-rsg-vms	Yes	VM running	Enabled for selected workspace	09/08/2023, 08:13:55	12	12	100%
lnvm02	dv4-Ind2-t-rsg-vms	Yes	VM running	Enabled for selected workspace	09/08/2023, 10:39:55	12	12	100%
WINVM03	dv4-Ind2-t-rsg-vms	Yes	VM running	Enabled for selected workspace	09/08/2023, 10:39:59	12	12	100%

The report as shown above is provided with some **filters [1]** to filter on:

- **TimeRange:** between last hour, last 90 days and even custom timerange
- **Subscription**
- Log Analytics **Workspace**
- **Servers**
- **Managed by Eviden:** if VM has EvidenManaged tag set to True
- **Powerstate** of the VM

Besides the filters, there is also a **search bar [2]** to filter on information that is not provided via a filter, like part of a VM name, (part of) resource group name or if Monitoring agent is Enabled for selected workspace.

In case the name of an application is in the VM name or in the resource group name this can be very useful.

For additional reporting or processing the data in excel the **Export to Excel [3]** option is available at the right top of the report

In the Virtual Machine column a **VM name [4]** can be selected to open the VM blade for that VM.

The data columns **Virtual Machine, Resource Group, Managed by Eviden** and **Powerstate** are **retrieved from Azure Resource Graph**. With this information it is possible to show also virtual machines that are stopped (VM deallocated) or that do not have the Monitoring agent provided or where the **Monitoring Agent** is connected to a log analytics workspace that is not selected in the **Workspace** filter.

The column **Monitoring Agent** shows information that is based on both the query data from Azure Resource Graph and the query data from log analytics. This is also why it is not possible to create a filter for this column. This column shows two possible values:

- **Enabled for selected workspace:** Means that the Monitoring agent extension is successfully provisioned to the virtual machine and is connected to one of the (in the filter selected) Log Analytics workspaces. If EvidenManaged tag is set for a VM and all workspaces (Eviden Landing Zones for Azure provides only one) are selected in the filter, "Enabled for selected workspace" would be shown in the report.
- **Not enabled (for selected workspace) or not working properly:** This means that there are 4 possible situations:
 - VM is not provisioned with monitoring agent. In most cases EvidenManaged tag is set to "No". If tag is set recently to "Yes" or VM is recently created it can take up to 12 hours before monitoring agent is provisioned to the VM!
 - VM is stopped. In Powerstate column "VM deallocated" is shown also
 - Monitoring Agent is connected to a loganalytics workspace that is not selected in the filter or is not connected to any loganalytics workspace. The best way to check if the VM is connected to any loganalytics workspace is to filter on VM name and select All for Workspaces.
 - Monitoring agent is not working properly and not providing (all) needed information to the loganalytics workspace.

In most of the "Not enabled .." situations some investigation is necessary to check if there is an issue and sometimes (re)installation of the monitoring agent or reconnecting with a loganalytics workspace is needed.

The columns **Last HeartBeat within time range**, **Available Hours**, **Total Hours** and **Availability** is retrieved through the log analytics workspace. **Last HeartBeat within time range** shows when VM was last seen on the log analytics workspace. This can be an indication when a VM is powered off (**Powerstate will be "VM deallocated"**) within the selected time range. If the VM is running a heartbeat will be received every minute.

To calculate the the availability percentage, the query divides the available hours with the total hours (set by TimeRange filter).

5. Performance workbook

The Performance report is used to provide performance information, for a time range, about virtual machines that are connected to a log analytics workspace.

At the top of this report there are 3 **filters [1]** to filter on **Subscription**, **Workspace** and to select the **Time Range** for the report. For Eviden Landing Zoned for Azure you should select the management subscription and the log analytics workspace that is used for the Eviden managed virtual machines.

Dashboard >

Performance ...

Azure Monitor

Workbooks Edit ? Help Auto refresh: Off

Performance Analysis

Subscriptions

Workspaces

Time Range

☒ Top 100 Machines
☐ Top 10 Machines

Computer Name Contain...

Counter

Aggregators

TableTrend

ResourceName ↑↓	Type	↑↓	Average	↑↓	P95th	↑↓	Max	↑↓	Trend (Average)	Properti...
linvm98	Azure Virtual Machine		2,629.35		2,643.434		2,643.434			Info
linvm87	Azure Virtual Machine		2,607.416		2,626.742		2,626.742			Info
linvm89	Azure Virtual Machine		2,515.369		2,533.738		2,533.738			Info
winvm87	Azure Virtual Machine		2,329.333		2,360		2,360			Info
winvm89	Azure Virtual Machine		2,308		2,415		2,415			Info
linvm99	Azure Virtual Machine		2,184.867		2,348.504		2,348.504			Info
winvm99	Azure Virtual Machine		2,124.667		2,289		2,289			Info
winvm98	Azure Virtual Machine		2,110.5		2,231		2,231			Info
winvm88	Azure Virtual Machine		2,057.5		2,190		2,190			Info

The report is divided into **2 tabs [2]**:

- The first tab "**top 100 machines**" shows some performance metrics of the top 100 machines.
- The second tab "**top 10 machines**" basically shows the same data but in graphs and only for the top 10 VM's.

Top 100 Machines tab

The top 100 Machines tab shows metrics for max 100 virtual machines based on the **filters [1]** at the top of this Performance report.

Top 100 Machines Top 10 Machines

Computer Name Conta...
Enter value

Counter
AvailableMB

Aggregators
3 selected

TableTrend
Average

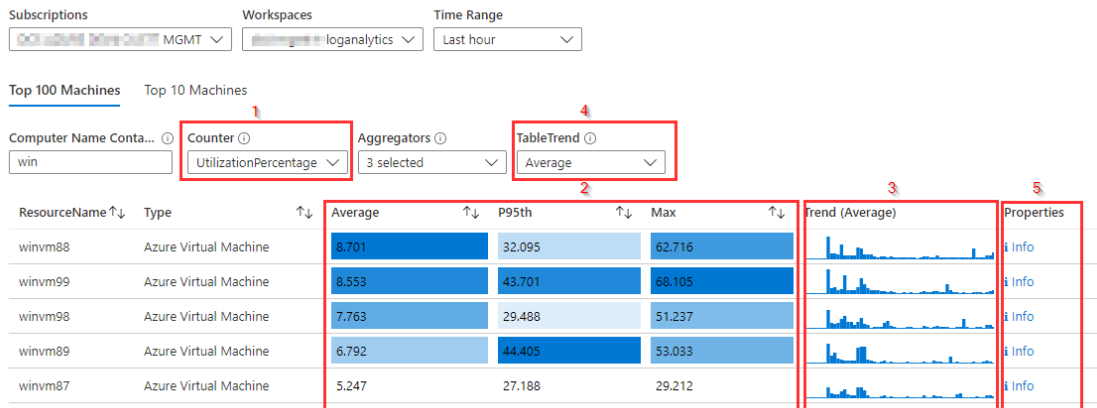
ResourceName ↑↓	Type	↑↓	Average	↑↓	P95th	↑↓	Max	↑↓	Trend (Average)	Properti...
linvm98	Azure Virtual Machine		2,629.35		2,643.434		2,643.434			i Info
linvm87	Azure Virtual Machine		2,607.416		2,626.742		2,626.742			i Info
linvm89	Azure Virtual Machine		2,515.369		2,533.738		2,533.738			i Info
winvm87	Azure Virtual Machine		2,329.333		2,360		2,360			i Info
winvm89	Azure Virtual Machine		2,308		2,415		2,415			i Info
linvm99	Azure Virtual Machine		2,184.867		2,348.504		2,348.504			i Info
winvm99	Azure Virtual Machine		2,124.667		2,289		2,289			i Info
winvm98	Azure Virtual Machine		2,110.5		2,231		2,231			i Info
winvm88	Azure Virtual Machine		2,057.5		2,190		2,190			i Info

The following filters are available:

- **Computer Name Contains:** This will filter the computer whose name contains the keyword.
- **Counter:** Select a VM performance counter that should be shown in the table. Only one counter can be selected, that can be a metric for Computer, Processor, Network, Logical disk or Memory.
- **Aggregators:** Select one or more aggregators to display in the table. Aggregators to select from are Average, P5th, P10th, P50th, P80th, P90th, P95th, Min, Max. At least one aggregator must be selected.
- **TableTrend:** Select a percentile to display in the Trend column in the table. Percentiles to select from are Average, P5th, P10th, P50th, P80th, P90th, P95th.

Based on the filters, an overview can be created for selected VM's on the selected metrics, like in the next picture for **utilization percentile [1]** in the last hour of the Windows VM's.

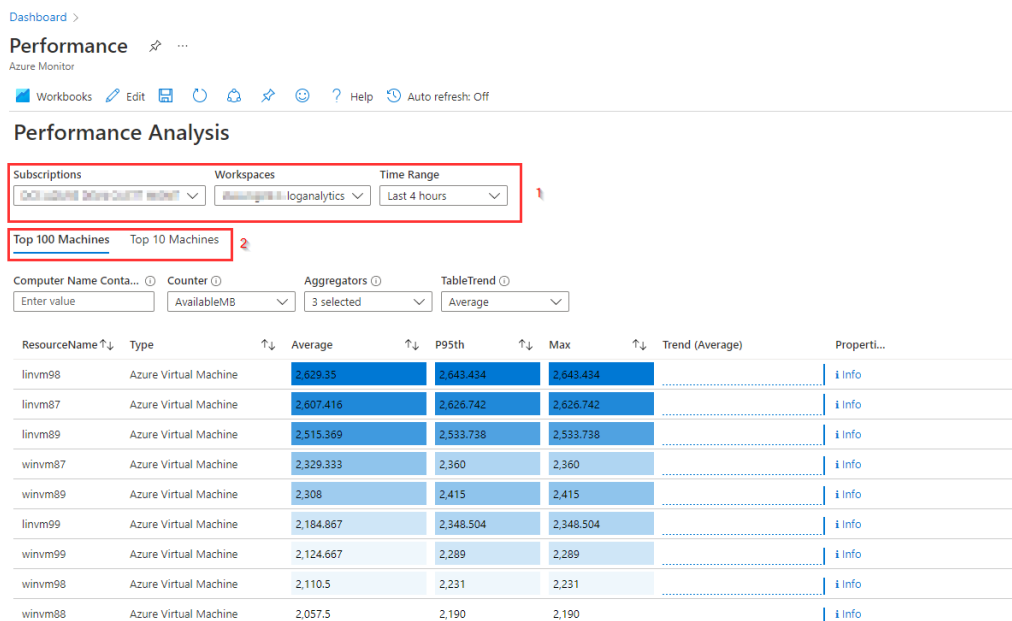
Performance Analysis



For this overview the aggregators **Average, P95th and Max** are selected [2]. When additional aggregators are selected, an additional column for this aggregator will be added to the table.

The **Trend column** [3] shows a small graphical overview of the trend for the percentage that is selected in the **Table Trend filter** [4]. This column provides a good indication about the trend within the selected time range. In the column for Trend the selected Table Trend percentile is displayed between curly brackets in the column name. By default, the average percentile is shown.

In the last column **Properties** [5] there is an info link available. Selecting this **Info link** [1] for a VM opens a **Details window** [2] with detailed hardware, network and operating system information for the selected VM, as shown in this picture:



8 April 2024

For internal use

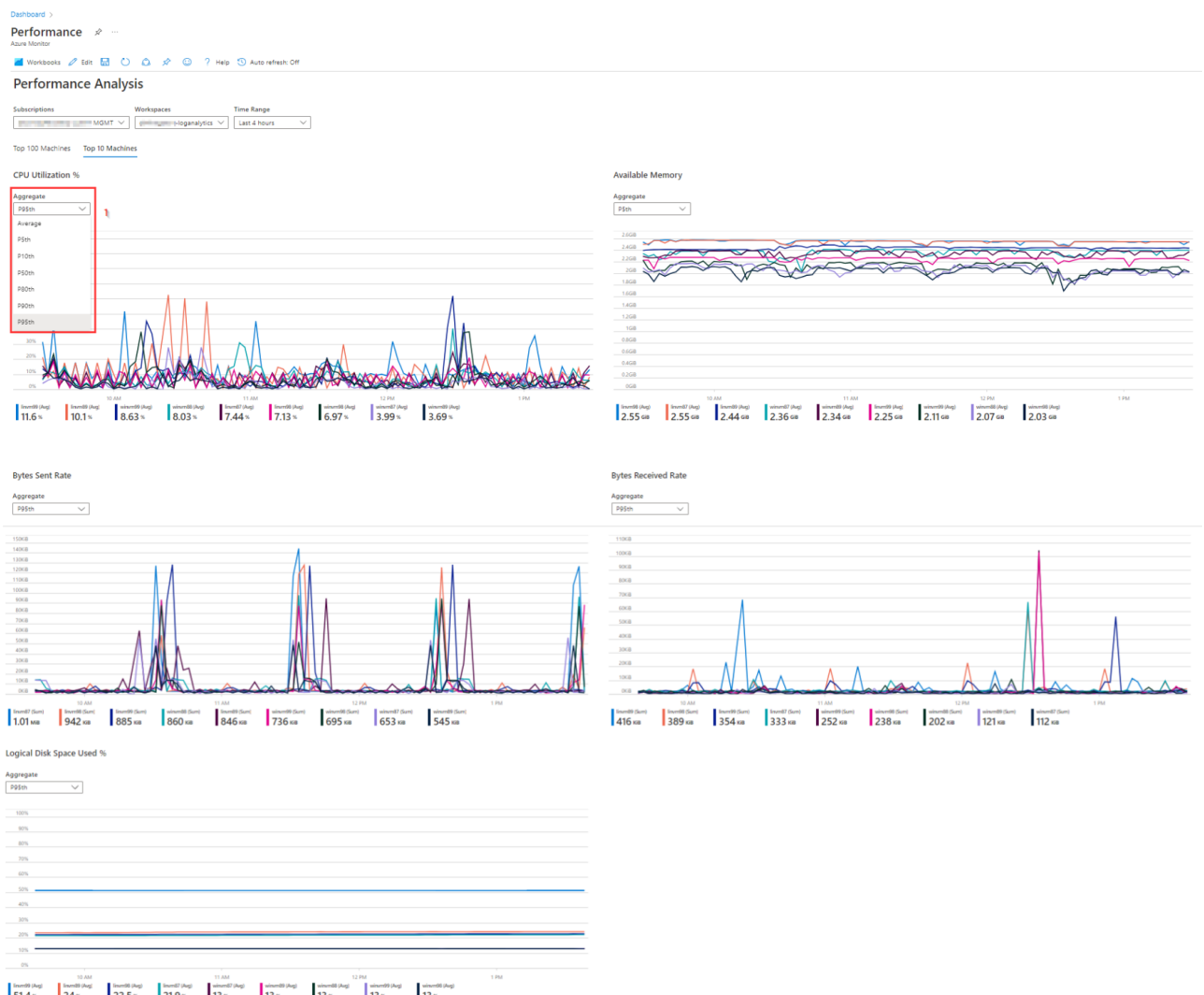
Version: 1.0

Top 10 Machines tab

The top 10 Machines tab shows metrics for max 10 virtual machines based on the filters at the top of this Performance report. In this tab a graphical overview is shown with the top 10 VM's for each of the following categories:

- CPU utilization %
- Available memory
- Bytes Send Rate
- Bytes Received Rate
- Logical Disk Space Used %

For each category it is possible to select the **percentile [1]** that will be shown in the graphical overview as shown in the picture.



8 April 2024

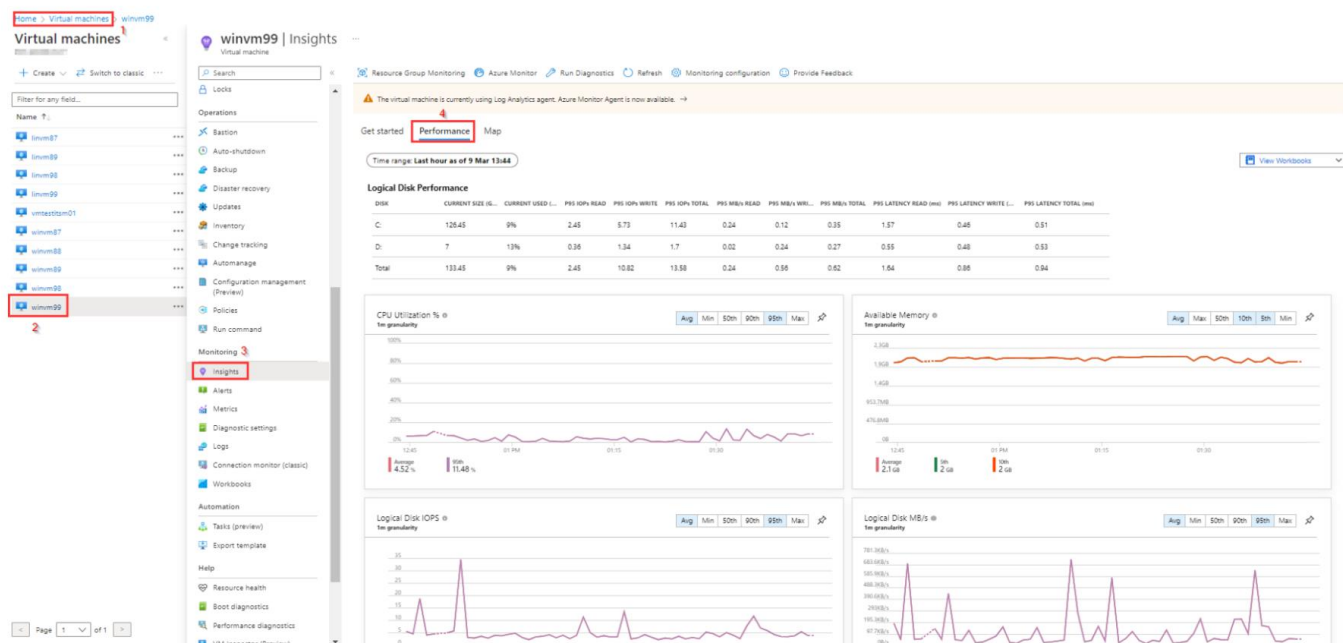
For internal use

Version: 1.0

As only the top ten is shown for each category its not possible to select a specific VM.

If these **graphics** are needed for a **specific virtual machine**, use the following steps:

- In Azure, find **Virtual Machines [1]** to get the overview of all virtual machines.
- Select the **Virtual Machine [2]** for which the performance metrics are required in a graphical overview.
- In the Virtual machine blade that opens click on the **Insights blade [3]**.
- Select the **Performance tab [4]** to view the graphics as shown in the picture.



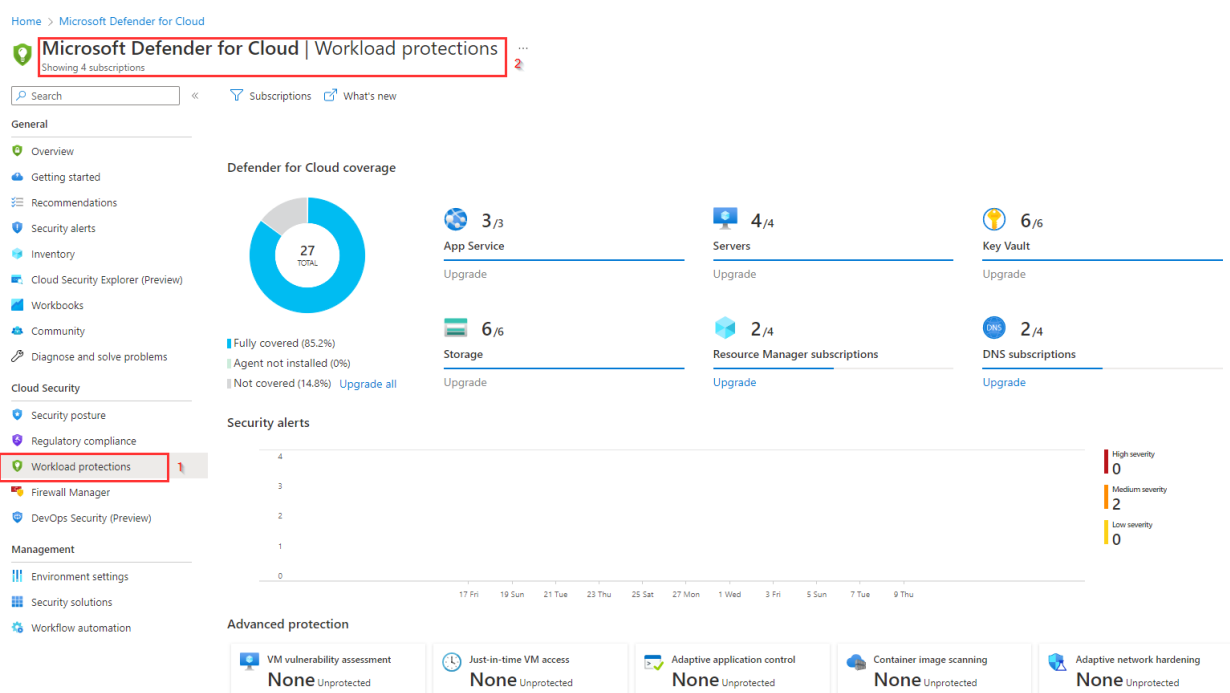
Important note: Insights and Diagnostic Settings must be enabled for the selected VM for this Performance tab to work.

6. Security Posture

The Azure Defender (within Security Center) native capabilities will be available by enabling Server licensing within Azure Defender and enables Azure Defender to support vulnerability assessment of VMs.

This leverages Microsoft's implementation of Qualys threat feeds to safeguard the security posture of managed VMs.

The Security Posture report is a tile that directs to **Workload Protections tab [1]** in the Azure Defender for **Cloud blade [2]**.



This Workload Protections tab is a dashboard that provides:

- Visibility into your Microsoft Defender for Cloud coverage across your different resource types.
- Links to configure advanced threat protection capabilities.
- The onboarding state and agent installation.
- Threat detection alerts.

This report is a native feature of Azure, so for more information about what is shown in this overview, please check [this link](#)

Note that not all VM's are applicable for Qualys.

7. VM OS Image gallery workbook

The VM OS Image Gallery report is used to provide an overview of the custom OS images that are provided to deploy VMs.

This report consists of 2 parts:

- An overview with shared image galleries and images that are available.
- Links to the Eviden Landing Zones for Azure Customer Guidance Documents.

At the top of the report there are several **filters [1]** to filter on Subscription, Shared Image Gallery, Image Name or OS Type that can be used to select a specific set of images.

VM OS Image Gallery ✱ ...

Azure Monitor

Workbooks Edit 🔍 🔄 🔔 🔗 📄 ? Help 🔄 Auto refresh: Off

Subscription	Shared Image Gallery	Image Name	OS type
All	All	All	All

Shared Image Gallery	ImageName	ImageVersion	OSType	ResourceGroup	OS Image Link	ResourceId
testGallery 2	Ubuntuthings	17.1.1	Linux	testGallery-17.1.1	testGallery/Ubuntuthings/17.1.1 3	/subscriptions/61c00000-0000-0000-0000-000000000000/resourceGroups/testGallery/providers/Microsoft.SharedImageGallery/images/17.1.1
testGallery	Ubuntuthings	17.1.0	Linux	testGallery-17.1.0	testGallery/Ubuntuthings/17.1.0	/subscriptions/61c00000-0000-0000-0000-000000000000/resourceGroups/testGallery/providers/Microsoft.SharedImageGallery/images/17.1.0
testGallery	Ubuntuthings	15.1.6	Linux	testGallery-15.1.6	testGallery/Ubuntuthings/15.1.6	/subscriptions/61c00000-0000-0000-0000-000000000000/resourceGroups/testGallery/providers/Microsoft.SharedImageGallery/images/15.1.6
testGallery	Windows2016CRM		Windows	testGallery-2016CRM	testGallery/Windows2016CRM	/subscriptions/61c00000-0000-0000-0000-000000000000/resourceGroups/testGallery/providers/Microsoft.SharedImageGallery/images/Windows2016CRM
SharedImageGalleryName	LinuxDef1		Linux	SharedImageGalleryName/LinuxDef1	SharedImageGalleryName/LinuxDef1	/subscriptions/61c00000-0000-0000-0000-000000000000/resourceGroups/SharedImageGalleryName/providers/Microsoft.SharedImageGallery/images/LinuxDef1
SharedImageGalleryName	SursImageDef1		Windows	SharedImageGalleryName/SursImageDef1	SharedImageGalleryName/SursImageDef1	/subscriptions/61c00000-0000-0000-0000-000000000000/resourceGroups/SharedImageGalleryName/providers/Microsoft.SharedImageGallery/images/SursImageDef1

By selecting a **shared image gallery [2]** in the **Shared Image Gallery** column you are redirected to the shared image gallery blade in Azure

The column **OS Image Link [3]** provides a direct link to the custom image and when selecting the link, the Image tab is opened, and you can click on "+ create VM" to create a VM using this image.

Dashboard > VM OS Image Gallery >

17.1.1 (testGallery/Ubuntuthings/17.1.1) ✱ ...

Image version | Directory: testGallery

Search (Ctrl+/) << + Create VM + Create VMSS Delete Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Update replication

Essentials

Resource group (change): testGallery-17.1.1

Status: Succeeded

Location: West Europe

Subscription (change): testGallery

Subscription ID: 61c00000-0000-0000-0000-000000000000

Tags (change): Click here to add tags

See more

Shared image gallery: testGallery

Image definition: Ubuntuthings

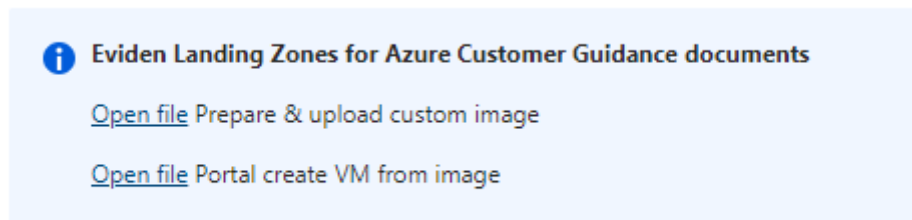
Replication status: Completed

Encryption type: Platform-managed key

End of life date: -

The column **ResourceId** opens a tab and the **ResourceId** can be copied and used it in an ARM template to create a VM based on the custom image.

The informational markdown text window at the bottom contains 2 links to the VM OS Image Gallery customer guidance documents, which are located in the artifacts repository storage container. There is one document for creating and uploading vhd image files and a 2nd document for creating VM's from images in the OS Image Gallery.



Clicking on either of the "open file" links will open a new tab with the document.

8. VM Tagging workbook

The VM Tagging report is used to provide an overview of all Eviden tags settings for all VM's to show per VM what features provided by Eviden are enabled or not.

Dashboard

VM Tagging

Azure Monitor

Workbooks Edit View Refresh Help Auto refresh: Off

Subscription	Virtual Machine	EvidenOsVersion	EvidenManaged	EvidenAntimalware	EvidenCompliance	EvidenBackup	EvidenPatching	EvidenEncryption	EvidenMaintenance
All	5 selected	All	All	All	All	All	All	All	Not set

Virtual Machine - Management tags overview

VM Name	Subscription	EvidenOsVersion	EvidenManaged	EvidenAntimalware	EvidenCompliance	EvidenBackup	EvidenPatching	EvidenEncryption	EvidenMaintenance	All tags overview
linvm01	[Icon] [Link]	LND2	Not Set	Yes	Not Set	Not Set	Linux-Dev	Not Set	Not Set	["EvidenPatching":"Linux-Dev","EvidenAntimalware":"true","EvidenPat"]
linvm02	[Icon] [Link]	LND2	Not Set	Yes	Yes	Not Set	Linux-Test	Not Set	Not Set	["EvidenAntimalware":"true","EvidenPat"]
linvm03	[Icon] [Link]	LND1	redhat 8.7	Yes	Not Set	Not Set	Gold	Linux-Dev	Not Set	["EvidenBackup":"Gold","EvidenPatchin"]
winvwm01	[Icon] [Link]	LND1	Not Set	Not Set	Yes	Not Set	Silver	windows-dev	Not Set	["EvidenAntimalware":"true","EvidenOS"]

In the top part the report provides several **filters [1]** to select the VM's to report on or to select VM's with a specific tag set (or not set). This way the filters at the top of the report can be used to get a clear overview which tag is set properly or not.

To change the value of a tag or define a tag, you can click on the **VM name [2]** in the report as this opens the blade for the selected VM and make the changed in the **VM overview blade**. It will take 10-15 seconds before the new value for a tag is visible in the report. You need to click on refresh to get the new value displayed in the report.

For an overview of all tags that are defined for a VM and the values that are set, in the last column **All Tags Overview [3]** is added. When clicking on this column for a particular VM a detailed overview of all tags defined for that VM is displayed.

9. Antimalware workbook

The Antimalware report provides an overview of the protection status of all VMs. The report consists of 3 parts:

- The top part provides a general overview of protection status for all VMs that potentially have antimalware capabilities.
- The middle part lists all VMs that have a protection status needing attention.
- The middle part provides an overview detected antimalware threats.

In the top part the report provides 2 **filters [1]**, one to select the subscriptions where the VM's reside to report on and one for the log analytics workspace where the VM's should be connected to. Though every workspace can be selected here, you should select the Eviden managed log analytics workspace in the management subscription.

Dashboard > Antimalware Azure Monitor

Workbooks Edit Auto refresh: Off

Subscription: All Log Analytics Workspace: All

VMs protection status

VM	Subscription	TypeOfProtection	ProtectionStatus	OS	AMProductVersion	SignatureVersion
linvm87		Defender Endpoint Protection for Linux	No real time protection	Linux	101.94.13	1.383.1215.0
linvm89		Defender Endpoint Protection for Linux	No real time protection	Linux	101.98.05	1.383.1215.0
linvm96		Defender Endpoint Protection for Linux	No real time protection	Linux	101.98.05	1.383.1215.0
linvm99		Defender Endpoint Protection for Linux	No real time protection	Linux	101.94.13	1.383.1266.0
winvms7		Windows Defender	Real time protection	Microsoft Windows Server 2016 Datacenter	4.18.2302.3	1.383.1335.0
winvms8		Windows Defender	Real time protection	Microsoft Windows Server 2019 Datacenter	4.18.2301.6	1.383.1335.0

VMs with Antimalware status needing attention

VM	Subscription	ProtectionStatus	TimeGenerated	ProtectionStatusDetails	ProtectionStatusRank
linvm87		No real time protection	3/9/2023, 3:35:08 PM	Real-time protection disabled;	270
linvm89		No real time protection	3/9/2023, 3:46:27 PM	Real-time protection disabled;	270
linvm96		No real time protection	3/9/2023, 3:35:00 PM	Real-time protection disabled;	270
linvm99		No real time protection	3/9/2023, 3:35:09 PM	Real-time protection disabled;	270

Detected Antimalware Threats

No antimalware threats found for VM's in selected subscription(s)

In the next section every part of the report is described.

The VMs protection status

The VMs protection status shows all VM's based on the selected filters and shows the Type of Protection together with the **ProtectionStatus [2]**. The ProtectionStatus shows if a VM is protected or not, while the TypeOfProtection shows the product that is used for antimalware. In the **AMProductVersion** and

SignatureVersion [3] of this part you find the version of the antimalware solution and the Signature Version.

To take action of get additional information on a specific VM you can select the **VM name [4]** in the VM column to be redirected to the blade for that VM.

VMs with Antimalware status needing attention

In the middle part of the report all VM's are shown that have a protection status set to one of the following:

ProtectionStatusRank	ProtectionStatus
450	Not Reporting
350	Action Required
270	No real time protection
250	Signatures out of date

This is fact a subset of the VM's shown in the top part where the **ProtectionStatus [5]** column is indicating that there is an issue with the antimalware protection state. More detailed information about the reason for this can be found in the columns **PortectionStatusDetails** and **ProtectionStatusRank [6]**.

As in the top part you can get additional information on a specific VM by selecting the VM name in the VM column to be redirected to the blade for that VM.

Detected Antimalware Threats

This bottom part of the report provides an overview of the antimalware threats that are detected in the selected subscription(s) and log analytics workspace. If there are no threats found, the message "**No antimalware threats found for VM's in selected subscription(s) [7]**" as shown in the picture will be displayed.

If one or more threats are found an overview is shown with the following columns:

- **VM:** showing the name of the VM where the threat is detected
- **Subscription:** the subscription in which the VM resides
- **AlertText:** the alert display name as is found in the log analytics workspace.
- **AlertTime:** the time the threat was first detected.
- **AlertUri:** a direct link to the alert details like e.g., threat and file information for a detected virus. Click on this link to be redirected to a webpage with more information about the threat found.

10. Availability Sets workbook

This report is used to make the status of an availability set visible and shows if the virtual machines that are part of an availability set are running. To show this the report consist of 2 parts:

- An overview of the availability sets
- An overview of the virtual machines in an availability set

10.1 Overview availability sets

In the upper part of the report there is an overview of all availability sets. It is possible to use the **filters [1]** at the top to filter on Availability set name, Subscription, Location, Status or if the Availability set is managed by Eviden.

Dashboard >

Availability Sets ✕ ...

Azure Monitor

Workbooks Edit View Refresh Help Auto refresh: Off

Name availability set	Subscription	Location	Status	Managed by Eviden
All	All	All	All	All

Overview availability sets

Availability Set	Subscription	Location	Resource Group	Update Domains	Fault Domains	# VM's	# VM's running	Status	Managed by Eviden
avset11	...	LND1	uksouth	5	2	2	2	Healthy	Yes
avset10	...	LND1	uksouth	5	2	1	1	Warning	Yes

The report shows an overview of the availability sets that are created, the configuration of the **availability set [2]** like the number of update domains and fault domains in the availability set, the number of virtual machines that are part of the availability set. In the column **#Vm's running [3]** you find the number of running virtual machines. Based on the number of VM's in the availability set compared to the number of Vm's running the **Status [4]** is determined.

Status can have the following values:

- **Healthy:** All virtual machines that are part of the availability set are running
- **Warning:** Not all virtual machines are running or there is only one virtual machine in the availability set.
- **Critical:** There is no running virtual machine in the availability set.
- **Unknown:** There is no virtual machine part of the availability set.

Status Unknown is possible when virtual machines were deleted that are part of an availability set and that the availability set still exists with no virtual machines. It is also possible to create an availability set with no virtual machines added to it.

So in this case it is possible that the availability set still need to be deleted or that there still need virtual machines to be added to the availability set

In the last column, **Managed by Eviden [5]**, is shown if the availability set is managed by Eviden or not.

10.2 Overview virtual machines in availability sets

For more detail about the virtual machines that are part of an availability set and the (power)state of the virtual machine, there is an overview of the virtual machines in the lower part of the report.

Name availability set	Resource group	OS	Powerstate	Managed by Eviden
All	All	All	All	All

Overview virtual machines in availability sets

VMName	AvailabilitySet	resourceGroup	OS	Powerstate	VM Managed by Eviden
linvm06	AVSET11		Not Set	running	Yes
linvm07	AVSET11		Not Set	running	Yes
winvm10	AVSET10		Not Set	running	Yes

In this overview you can **filter[1]** on availability set, Resource group, Operating System, Powerstate and if the virtual machine is managed by Eviden (tag **EvidenManaged** is set to "**true**").

In case a virtual machine is not running in column **Powerstate [2]** "**deallocated**" is shown.

To change the powerstate of a virtual machine, you can click on the **VM name [3]** in the report to be redirected to the VM blade and make the change in the VM overview blade. It will take 10-15 seconds before the new status is visible in the report. You need to click on refresh to get the new status displayed in the report.

11. Scale Sets workbook

This report is used to show an overview of all scale sets, makes the status of a scale set visible and shows if the virtual machine instances that are part of a scale set are running.

In Azure, there are two orchestration modes for scale sets that can be set at creation time :

- Flexible mode (it's now the default since November 2023)

Flexible Orchestration is the new default model of managing VMs in a scale set.

Achieve high availability at scale with identical or multiple virtual machine types.

VM are managed as normal VMs by Azure, and can be added to the ScaleSet after creation.

- Uniform mode

Uniform Orchestration is the traditional model of managing VMs in a scale set. Optimized for large-scale stateless workloads with identical instances.

Because those two modes have different management APIs, the details part of the report is split in two parts to show the details of the instances for each orchestration mode.

This report consist of 3 parts:

- An overview of scale sets
- Scale sets Details For Flexible mode
- Scale sets Details For Uniform mode

11.1 Overview scale sets

In the upper part of the report there is an overview of all scale sets. It is possible to **filter [1]** on Scale Set Name, Subscription, Location, Scaling, Upgrade Policy, OS, Status or if the Scale Set is Managed by Eviden.

Dashboard > Scale Sets

Azure Monitor

Workbooks Edit Help Auto refresh: Off

Scale Set Name	Subscription	Location	Scaling	UpgradePolicy	OS	Status	Managed by Eviden
All	All	All	All	All	All	All	All

Overview scale sets

Scale Set	Subscription	Location	Resource Group	OrchestrationMode	Scaling	Fault Domains	OverProvision	Placementgroups	Upgrade Policy	OS	# Instances	# Instances running	Status	Managed by Eviden
winad02	AKS Azure DevOps	uksouth	aks-aks-aks-aks	Flexible	Manual	1	Disabled	Multiple	Manual	Windows	3	3	Healthy	Yes
winad01	DCS AZURE DEV4 CUSTY UNDT	uksouth	aks-aks-aks-aks	Uniform	Manual	1	Disabled	Multiple	Manual	Windows	2	0	Critical	No

The report shows an **overview of the scale sets** that are created with their **configuration settings [2]** like:

- **OrchestrationMode:** Show the orchestration mode (Flexible or Uniform)
- **Scaling:** if **custom auto-scale** is defined or **manual scaling**
- **Fault Domains:** the number of fault domains in the scale set
- **Overprovisioning:** shows if **overprovisioning** is enabled or disabled
- **Placementgroups:** if a single- or multiple **placementgroups** are used
- **Upgrade Policy:** is manual, automatic or N/A. As upgrade modes are not supported for Virtual machine scale sets with flexible orchestration mode, Upgrade Policy will show N/A.
- **OS:** shows if Scale set is Windows or Linux
- **# Instances:** the number of virtual machines instances that are part of the scale set

Beside this configuration information there is a column **#Instances running [3]** to show the number of VM instances that are active and a **Status [4]** column that shows the status of the scale set based on the number of instances in the scale set compared to the number of scale set instances running.

Status can have the following values:

- **Healthy:** All virtual machine instances that are part of the scale set are running
- **Warning:** Not all virtual machine instances are running or there is only one virtual machine instance in the scale set.
- **Critical:** There is no running virtual machine instance in the scale set.
- **Unknown:** There is no virtual machine instance part of the scale set.

Status Unknown is possible when virtual machine instances were deleted that are part of a scale set set and that the scale set still exists with no virtual machine instances.

The last column **Managed by Eviden** shows if the scale set is **managed by Eviden**.

If the availability set has the tag **EvidenManaged** set to **true** then the column **Managed by Eviden** shows **Yes** in the report.

To show more details of a scale set or change the powerstate of an instance, you can click on the **Scale Set name [6]** in the report to be redirected to the scale set blade and make the changes for the scale set.

11.2 Scale Set Details (Flexible mode and Uniform mode)

For more detail about the virtual machine instances that are part of a scale set, there is an **overview of a specific scale set** in the second part of the report for each Orchestration mode.

Subscription

Resource Group

Scale Set Name

Any one

Any one

wins02

Scale Set Details

Name	ComputerName	InstanceId	Location	Tags	SKU	OSPublisher	OSVersion	ProvisioningState	Priority	Availability Zone (if configured)
wins02_0	wins02by000000	wins02/0	uksouth	[{"evidenmanaged":true}]	Standard_DS1_v2	MicrosoftWindowsServer	2016-datacenter-gensecond	Succeeded		[1]
wins02_1	wins02by000001	wins02/1	uksouth	[{"evidenmanaged":true}]	Standard_DS1_v2	MicrosoftWindowsServer	2016-datacenter-gensecond	Succeeded		[1]
wins02_2	wins02by000002	wins02/2	uksouth	[{"evidenmanaged":true}]	Standard_DS1_v2	MicrosoftWindowsServer	2016-datacenter-gensecond	Succeeded		[1]

<div>Instance</div> <div>1</div>												
Scale Sets Instance Details (ComputerName only visible when instance is powered on)												
ComputerName	OSVersion	PlatformFaultDomain	ProvisioningState	PowerState								
wins02by000001	Windows Server 2016 Datacenter		0 Provisioning succeeded	VM running								

In this overview you can **filter [1]** on Subscription, Resource group and Scale Set Name to select a specific scale set. Using these filter only one scale set can be selected at once.

In this overview the instances for the selected scale set are shown with the **Name**, **ComputerName**, **InstanceId** and with its **configuration information [2]** like **SKU**, **OSPublisher** and **OSVersion**.

There is also a column with the **Provisioning State [3]**, the **Priority [2]** (if any configured) and the **Availability Zone [5]**

To show more details of an instance or to delete an instance, you can click on the **InstanceId [6]** in the report to be redirected to the instance blade.

Known issues.

In case an **instance** is **not powered on**, the report is not able to show the **ComputerName** and the **OSVersion** of an instance.

The **status** in the upper part of the report is not updated real-time. It can take up to several minutes before the status is updated after a change in the **number of (running) instances**.

12. Disk Encryption workbook

The Disk Encryption workbook provides an overview of Disk Encryption settings and status for VMs and their associated disks in the Azure environment. The report consist of 2 parts:

- The first part at the top provides an overview of all VM's with encryption configuration and powerstate.
- The bottom part shows an overview of each disk for a VM and the (encryption) status and settings.

At the top of the report **filters [1]** are available to select on Subscription, VM name, Resource group and EvidenEncryption tag value.

Subscription	Resource group	Virtual Machine	EvidenEncryption (1)
All	All	3 selected	All

VM	Resource group	Location	Subscription	Encryption at host	EvidenEncryption tag	Power state
vm001	dk4-ind2-n-rig-vm	ukouth	DCS AZURE DEV4 CUST7 UN02	No	No	VM running
vm001	dk4-ind1-n-rig-vm	westeurope	DCS AZURE DEV4 CUST7 UN01	No	Yes	VM running
vm008	dk4-ind1-n-rig-vm	ukouth	DCS AZURE DEV4 CUST7 UN01	No	Yes	VM running

VM name	VM	Disk	Disk encryption	Encryption at host	ADE enabled	EvidenEncryption tag	Attention	Disk encryption set	Key vault	Disk size GB	Disk SKU	Disk state
vm001 (1)	vm001	vm001_OsDisk_1_2b1c1279b0d4	SSE with PMK	No	No	Yes	EvidenEncryption set, but SSE-PMK detected.			10	Premium_LRS	Attached
vm001 (1)	vm001	vm001_OsDisk_1_206119a878f5	SSE with CMK	No	No	Yes		dk4-ind1-n-rig-vm-ks	dk4-ind1-n-rig-vm-ks	127	Premium_LRS	Attached
vm008 (1)	vm008	vm008_OsDisk_1_6b3d4e4d114	SSE with PMK	No	No	Yes	EvidenEncryption set, but SSE-PMK detected.			127	Standard_LRS	Attached

At the top part of the report all VM's based on the filter settings are shown with the setting for **Encryption at host [2]**, **EvidenEncryption tag [3]** and the **Power state [4]**.

When the **EvidenEncryption** tag is set to "Yes", this means that the disks of the VM will be encrypted with a customer managed key using the disk encryption set that is provided by the keyvault for the location of the VM.

Encryption at host means that the encryption starts on the VM host itself, the Azure server that your VM is allocated to. For more information about encryption at host, check this [link](#).

In the bottom part of the report the disks with encryption settings, grouped by VM are shown. Besides the columns, already shown in the top part also, there are additional columns with information for each disk of a VM shown.

In the **Disk encryption [6]** column the type of disk encryption is shown. this can be using Platform-managed keys (**SSE with PMK**) or with Customer-managed keys (**SSE with CMK**). for more information check this [link](#) .

The **ADE enabled [7]** column shows if Azure Disk Encryption (ADE) is enabled or not. For more information about ADE for Windows and Linux Disks check this [link](#) .

In the **Attention [8]** column is shown if there are any issues detected with the disk encryption.

Depending on value set for **EvidenEncryption** tag, settings needing attention are indicated:

- Disks with ADE (Azure Disk Encryption) enabled, cannot be encrypted SSE-CMK. So desired state for EvidenEncryption=true cannot get achieved.
- Disk encrypted at-rest with SSE-PMK differ from EvidenEncryption=true setting. SSE with CMK is then not possible.
- Invalid tag value for EvidenEncryption tag

For disks encrypted at-rest with Customer Managed Keys (SSE with CMK), the associated **Disk Encryption Set and Key Vault [9]** is included.

The **last 3 columns [10]** show the settings for the disk it selves, like **Disk size** in GB, **Disk SKU** and **Disk state**.

13. Storage Accounts workbook

This report is used to make the configuration (including kind and SKU), status and workload of a Storage Account visible. The report has 2 parts, as already mentioned:

- Storage account Configuration Overview
- Storage Account Workloads

13.1 Storage account Configuration Overview

In the top part it is possible to **filter [1]** on **Subscription**, **Resource Group**, **Kind** and if the Storage Account is **managed by Eviden**.

Dashboard >

Storage Accounts Auto refresh: Off

Workbooks Auto refresh: Off

Storage Account Configuration Overview

Subscription	Resource Group	Kind	Managed by Eviden
All	All	All	All

Name	Subscription	ResourceGroup	Location	Kind	SKU Name	Public Access	Access Tier	EvidenPurpose	EvidenManaged	Status
aks-fcrfordevelopdiag	AKS-UK-SUBSCRIPTION	LND1	uksouth	Storage	Standard_LRS	true		-	No	available
aks-fcrfordevdiag	AKS-UK-SUBSCRIPTION	LND1	uksouth	Storage	Standard_LRS	true		-	Yes	available
aks-fcrfordevdisks	AKS-UK-SUBSCRIPTION	LND1	uksouth	Storage	Standard_LRS	true		-	Yes	available
aks-fcrfordevdisks216	AKS-UK-SUBSCRIPTION	LND1	uksouth	Storage	Premium_LRS	true		-	Yes	available
aks-fcrfordevdisks347	AKS-UK-SUBSCRIPTION	LND1	westeurope	Storage	Standard_LRS	false		-	No	available
aks-fcrfordevdisks4566df	AKS-UK-SUBSCRIPTION	LND1	westeurope	Storage	Standard_LRS	true		-	No	available
aks-fcrfordevdisks558	AKS-UK-SUBSCRIPTION	LND2	westeurope	StorageV2	Standard_LRS	false	Hot	-	No	available
aks-fcrfordevdisks122dd	AKS-UK-SUBSCRIPTION	MGMT	westeurope	StorageV2	Standard_LRS	false	Hot	-	No	available
aks-fcrfordevdisks0245118042	AKS-UK-SUBSCRIPTION	MGMT	westeurope	StorageV2	Standard_LRS	false	Hot	-	No	available
aks-fcrfordevdisks30775nw	AKS-UK-SUBSCRIPTION	MGMT	uksouth	StorageV2	Standard_LRS	false	Hot	-	No	available
aks-fcrfordevdisks30775nw	AKS-UK-SUBSCRIPTION	MGMT	uksouth	StorageV2	Standard_LRS	false	Hot	-	No	available

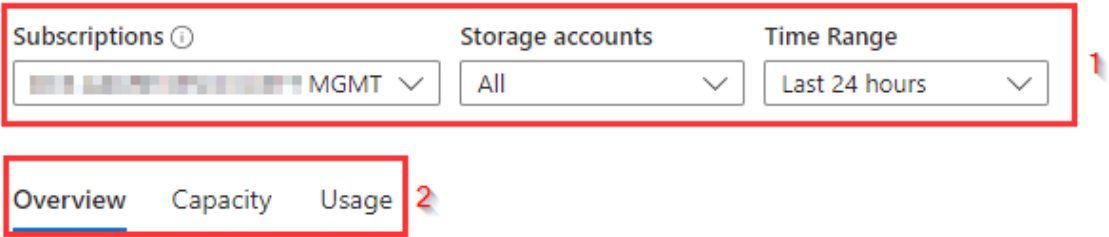
The report shows an **overview of the Storage Accounts** that are created with their **configuration [2]** like **Kind**, **SKU**, **Public Access** and **Access Tier**. In the **EvidenPurpose [3]** column is visible if the EvidenPurpose tag is set to a specific value that indicates the purpose of the storage account for ELZ Azure. The **EvidenManaged [4]** column show if the storage account is managed by Eviden. If so the value in this column is set to **Yes**. The **Status [5]** column shows if the storage accounts is currently available for access.

For more detail about a storage account is is possible to select the **name of the Storage Account [6]** in the **Name** column to open the **Storage Account blade**.

13.2 Storage Accounts Workloads

The bottom part of the Storage account report provides workload data based on the Azure Metrics for Storage Accounts. For the Storage Accounts Workloads it is possible to **filter [1]** on Subscriptions, Storage Accounts and Time Range.

Storage Account Workloads



The Storage Accounts Workloads reporting part consists of **3 blades [2]**:

- Overview
- Capacity
- Usage

Below the parts are described in more detail

13.3 Storage Accounts Workloads Overview blade

For the selected subscriptions and storage accounts the **Overview blade** shows for the storage accounts, that are grouped by **Subscription [1]** in the first column, the **Average Availability [2]**, **Transactions and Transactions Timeline [3]** (shows in brief when transactions occur), **E2E Latency, Server Latency and Errors [4]** that had occurred during the selected time range.

Subscriptions ⓘ Storage accounts Time Range

MGMT All Last 24 hours

Overview Capacity Usage

This overview dynamically displays the error information columns based on errors that occurred in the selected time range.

For more detailed information about the E2E Latency, Server Latency or Errors you can click on the displayed values to open a more detailed overview for a specific Storage Account

Subscription ⓘ	Availability (Average) ⓘ	Transactions ⓘ	Transactions Timeline ⓘ	E2E Latency ⓘ	Server Latency ⓘ	ClientOtherError/Errors ⓘ
MGMT (1)	130.2K					
...	100 %	52.6K		8.24ms	4.91ms	5.6K
...	100 %	19.5K		12.3ms	4ms	4.4K
...	100 %	5.9K		12.63ms	9.62ms	2.4K
...	100 %	4.9K		13.68ms	8.87ms	2.1K
...	100 %	6.8K		14ms	10.67ms	2.5K
...	100 %	6.2K		14.52ms	5.97ms	2.6K
...	100 %	6.5K		14.86ms	8.72ms	2.6K
...	100 %	5.2K		14.87ms	9.06ms	2.3K
...	100 %	5.9K		15.34ms	9.51ms	2.5K

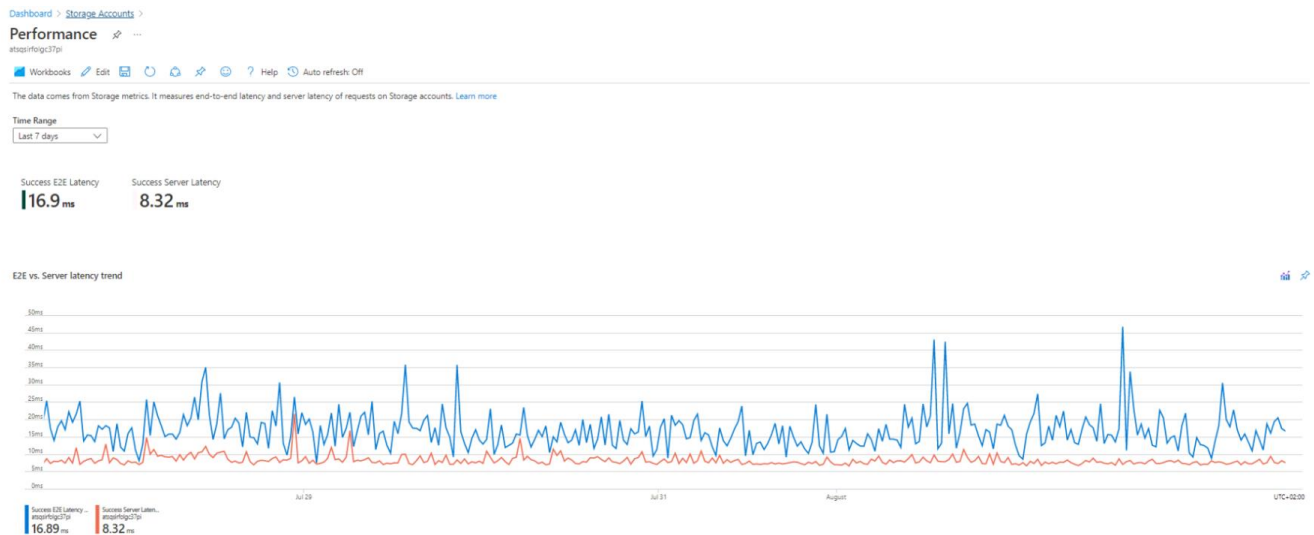
In the right corner of the Overview Blade there is an option to **export [5]** the Overview data to Excel

For more detail about the Storage Account it selves you can click on the **Storage Account name [6]** to be redirected tot the overview blade for the specific Storage Account.

If more detailed information is needed about the E2E Latency, Server Latency or

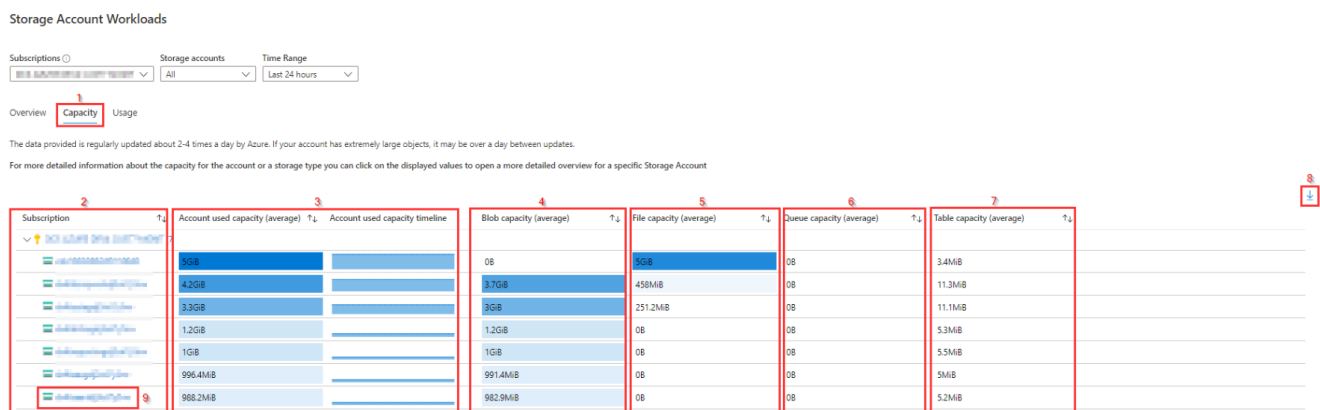
one of the error columns, you can click on the displayed value in the respective **column [4]** for the storage account to get more detailed (graphical) information for the selected Storage Account in the selected time range.

Below is an example of the E2E latency and Server latency for a Storage Account when the value in the E2E Latency or Server Latency column is selected.



13.4 Storage Accounts Workloads Capacity blade

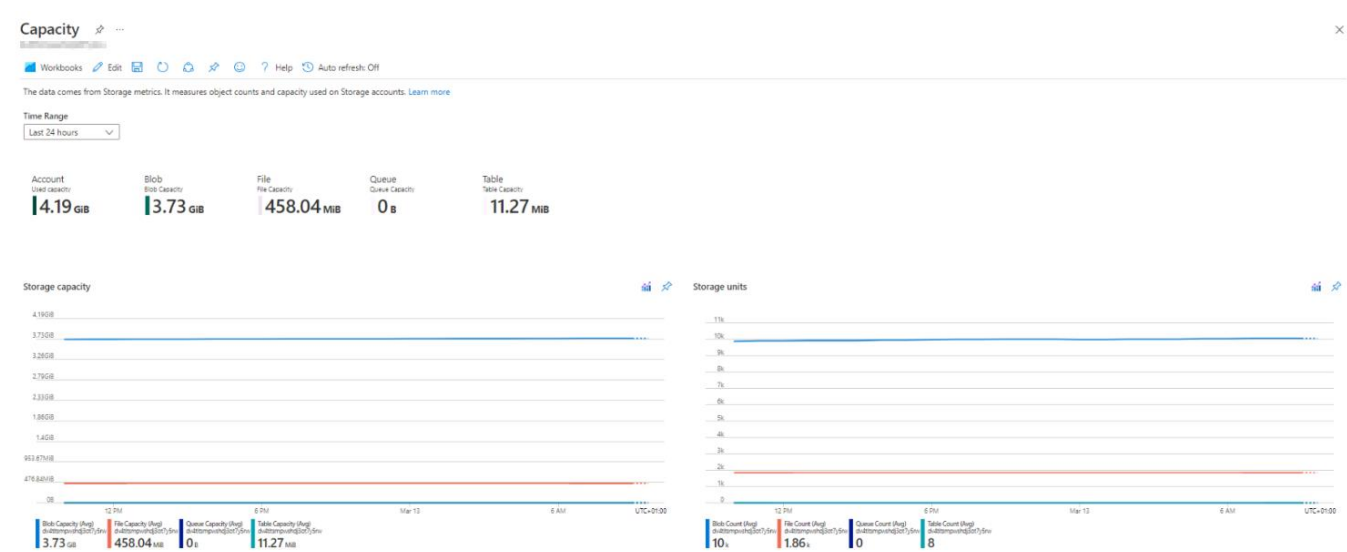
For the selected subscriptions and storage accounts the **capacity blade [1]** shows for the storage accounts, that are grouped by **Subscription [2]**, the **Average used Account capacity and the Account used capacity timeline [3]**, **average Blob capacity [4]**, **average File capacity [5]**, **average Queue capacity [6]** and **average Table capacity [7]** within the selected time range.



In the right corner of the Capacity Blade there is an option to **export [8]** the Capacity data to Excel.

For more detail about the Storage Account it selves you can click on the **Storage Account name [9]** to be redirected tot the overview blade for the specific Storage Account.

If more detailed information is needed about the capacity displayed in the report, you can click on one of the displayed values in the columns for the average capacity to get more detailed (graphical) information for the selected Storage Account in the selected time range.
Below is an example of the used capacity for a Storage Account when the value in the Account used capacity, Blob capacity, File capacity, Queue capacity or Table capacity column is selected.



13.5 Storage Accounts Workloads Usage blade

For the selected subscriptions and storage accounts the **Usage blade [1]** shows for the storage accounts, that are grouped by subscription [2], the **average count of Blob containers, Blobs, Files Shares, Files, Queues, Queue Messages, Tables and Table entities [3]** during the selected time range.

Storage Account Workloads

Subscriptions: [2] Storage accounts: [3] Time Range: Last 24 hours

Overview Capacity **Usage [1]**

The data provided is the average for the selected time range and regularly updated about 2-4 times a day by Azure. If your account has extremely large objects, it may be over a day between updates.
For the most recent metrics click on a Storage Account Name and then select the Storage Browser tab.

Subscription [2]	Blob Container Count (Average) [4]	Blob Count (Average) [4]	File Share Count (Average) [4]	File Count (Average) [4]	Queue Count (Average) [4]	Queue Message Count (Average) [4]	Table Count (Average) [4]	Table Entity Count (Average) [4]
Subscription 1	0	0	1	1	0	0	5	1,048
Subscription 2	11	7,288	0	0	0	0	8	1,616
Subscription 3	8	9,998	1	1,659	0	0	8	3,436
Subscription 4	9	9,970	1	1,030	0	0	8	3,396
Subscription 5	14	6,695	0	0	0	0	8	1,670
Subscription 6	7	6,540	0	0	0	0	8	1,602
Subscription 7	9	6,508	0	0	0	0	8	1,531

In the right corner of the Usage Blade there is an option to **export [4]** the usage data to Excel.

For more detail about the Storage Account it selves you can click on the **Storage Account name [5]** to be redirected tot the overview blade for the specific Storage Account. In the **Storage Browser blade** you can then find more detailed information about the storage usage for the Storage Account.