EVIDEN
an atos business

For internal use

# EVIDEN LANDING ZONES FOR AZURE CLOUD CORE DASHBOARD AND WORKBOOK INSTRUCTION MANUAL

| | | |
|---|---|---|
| **Author(s)** | : | **Klaas Jan de Jager** |
| **Version** | : | **1.0** |
| **Status** | : | **Final** |
| **Source** | : | **Eviden Landing Zones for Azure** |
| **Document date** | : | **27 November 2023** |
| **Number of pages** | : | **50** |

EVIDEN
an atos business

# Contents

EVIDEN
an atos business

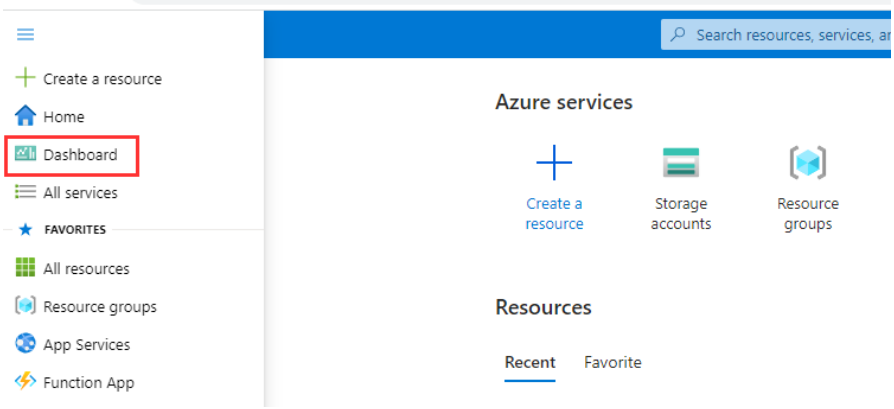
# List of changes

| Version | Date | Description | Author(s) |
|---|---|---|---|
| 0.9 | 22-08-2023 | Draft Eviden version | K.J. de Jager |
| 1.0 | 31-10-2023 | Initial Eviden version | K.J. de Jager |
| | | | |

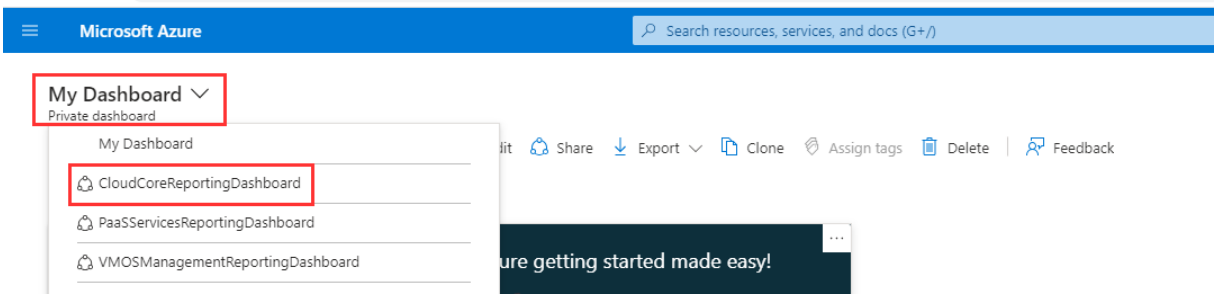
# 1. Eviden Landing Zones for Azure Cloud Core Reporting Dashboard

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, Workbook, or Storage Account Container. These tiles are grouped by category namely, IAM, Operational, Policy, and Financial. You can scroll up and down through the dashboard to see all groups and 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.

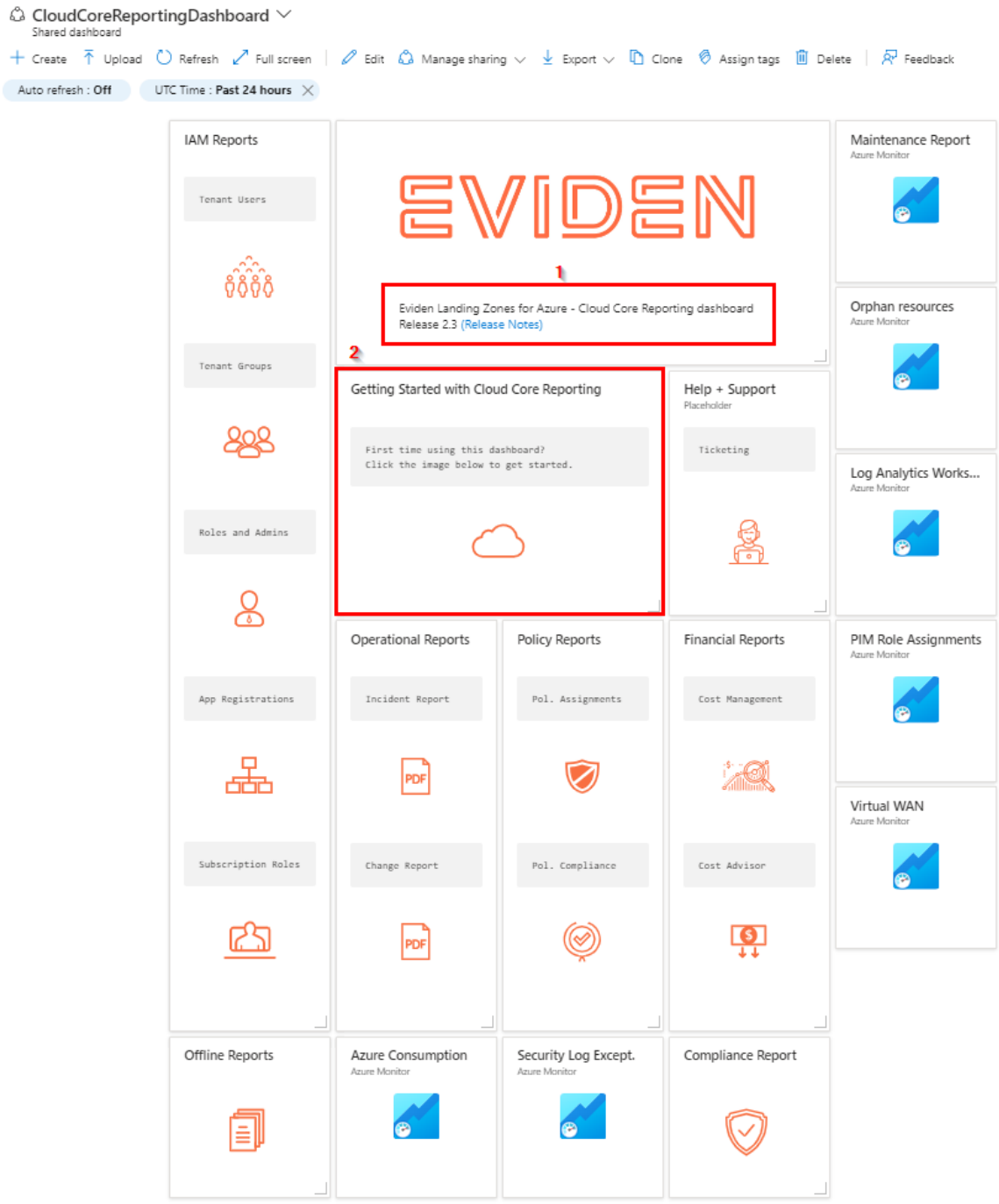



This should directly send you to the correct dashboard. If this is not the case, change the dashboard add the left top corner by clicking on the dashboard title and select CloudCoreReportingDashboard, see image below.




**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 Cloud Core Reporting dashboard, as in the picture below, now appears:




In the text under the **Eviden Logo [1]**, you will find the version of Eviden Landing Zones for Azure that is deployed.

At the next line you find a link to the *Release notes* that will redirect to the Eviden Landing Zones for Azure  release notes page.

The tile **“Getting Started with Cloud Core Reporting” [2]** redirects you to the up-to-date version of the getting started manual (this document) that is part of the release as displayed underneath the logo.

In the following paragraphs all other tiles and workbooks that are part of this dashboard will be shortly described.

# 2. IAM Reports

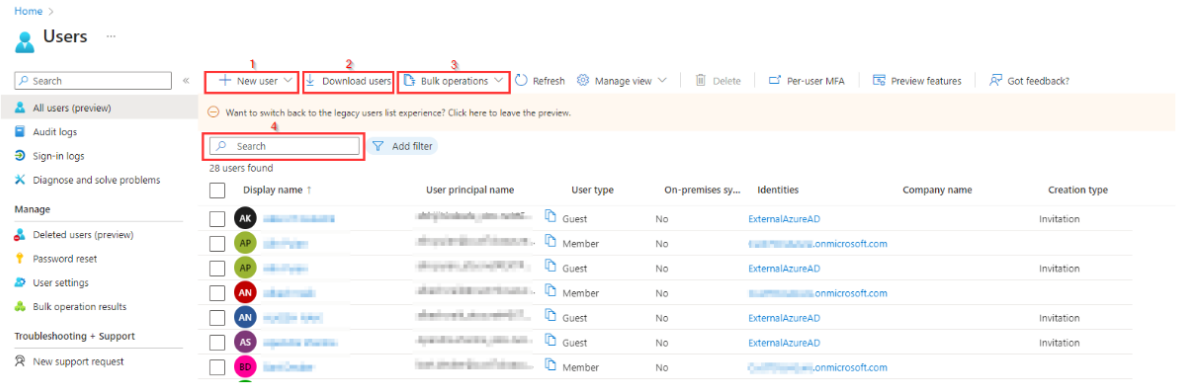
IAM Reports is a section in the dashboard that consists of 5 tiles that contains a link to redirect you to an Azure blade where the respective reports can be found:

- Tenant Users: Customer Tenant Azure AD Users
- Tenant Groups: Customer Tenant Azure AD Groups
- Roles and Admins: Customer Tenant Azure AD Roles (such as global admin or many others: Users or Groups are added to Roles to be granted AD-level rights)
- App Registrations: Customer Tenant Azure AD App Registrations to create registrations for applications and assign permissions accordingly.
- Subscription Roles: Per customer subscription IAM Roles (such as subscription owner, contributor, etc...: Users or Groups are added to roles to be granted subscription-level rights)

These reports provide details on identity and access management in Azure, like users, groups, roles and app registrations defined within the customer subscription(s). For this report it is key to have a clear overview of the users and roles. For a detailed description about Azure AD, check this link.

## 2.1 IAM Reports – Tenant Users

The Tenant Users tile in the dashboard redirects you to the Azure Active Directory Users blade in the customer environment:



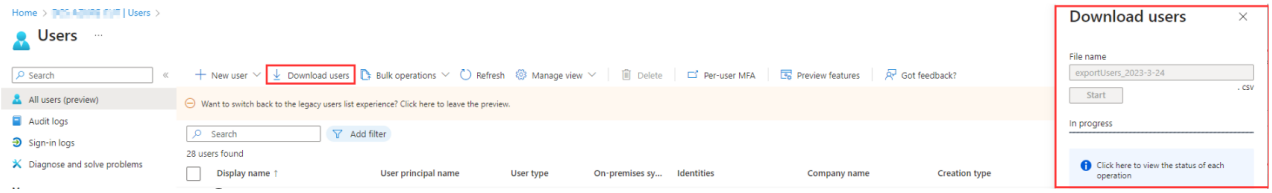

In the 'users blade' the Azure active directory users can be managed like creating a **New user [1]**, **Download users overview [2]** or perform **Bulk operations {3]** on users.

**New User[1]** has two options:

- *Create new user*: Create a new internal user in your organisation.
- *Invite external user*: Invite an external user to collaborate with your organisation.

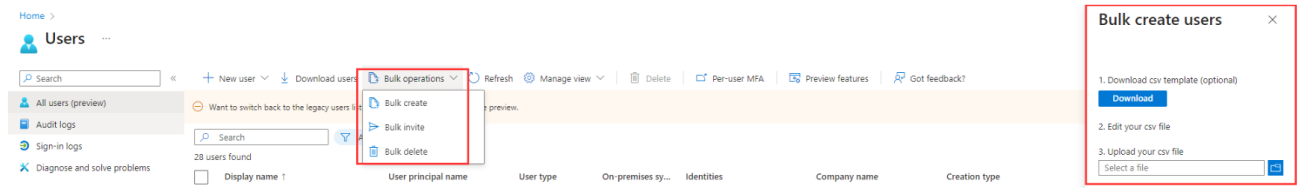
For more information about both options, check this link

**Download users [2]** is a good feature to create a report on all users if there are a lot of users created already. By selecting Download users a windows is opened at the right top of the blade:




In this window the proposed file name can be changed and after **Start** is selected a csv will be created. If the creation of the csv file is succeeded, you will get the option to download the file.

**Bulk operations {3]** is a nice feature to create a lot of users at once. This is especially handy right after the customer environment is deployed and all customer users need to be added to Azure AD.
This feature can also be used for **Bulk invite** or **Bulk delete** of users.
For the bulk options a **CSV template** need to be created and uploaded to Azure:



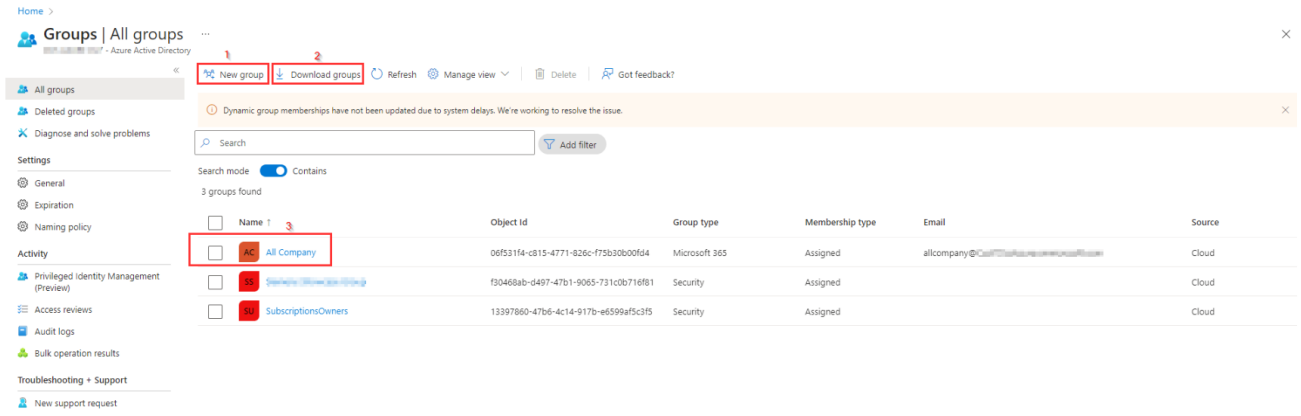

More information about bulk operations can be found here:

- Create users in bulk
- Delete users in bulk

**Bulk import service limits:** Each bulk activity to create users can run for up to one hour. This enables bulk creation of at least 50,000 users.

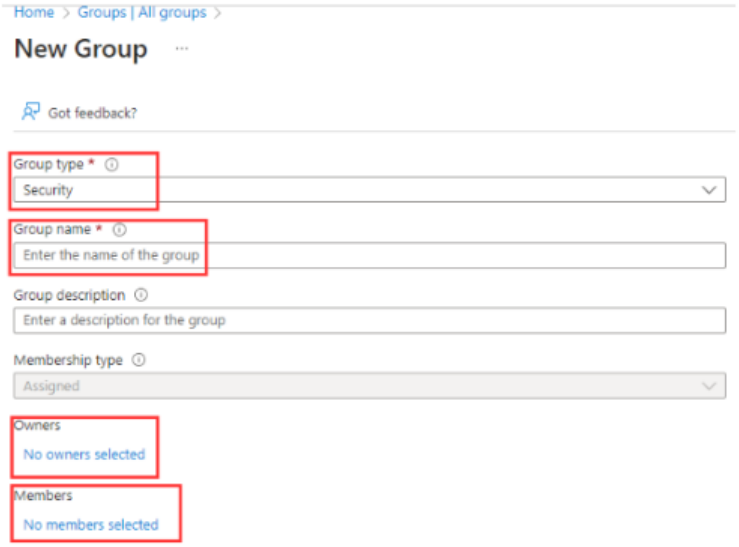
## 2.2 IAM Reports - Tenant Groups

The Tenant Groups tile in the dashboard redirects you to the Azure Active Directory Groups blade in the customer environment:




In this groups blade the Azure active directory groups can be managed like creating a **New group [1]** and **Download groups overview [2]**.

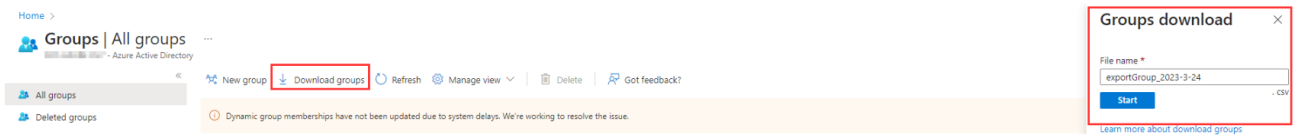
**New group [1]** opens a separate window to create a new group by selecting the Group type (Security or Microsoft 365), the Groups name and assign Owners and Members to the new group.




By selecting an **existing group [3]** this groups can be managed, like adding users to or removing users from this group or add/remove Azure role assignments.

For more information about the creation of groups or manage the groups check this link .

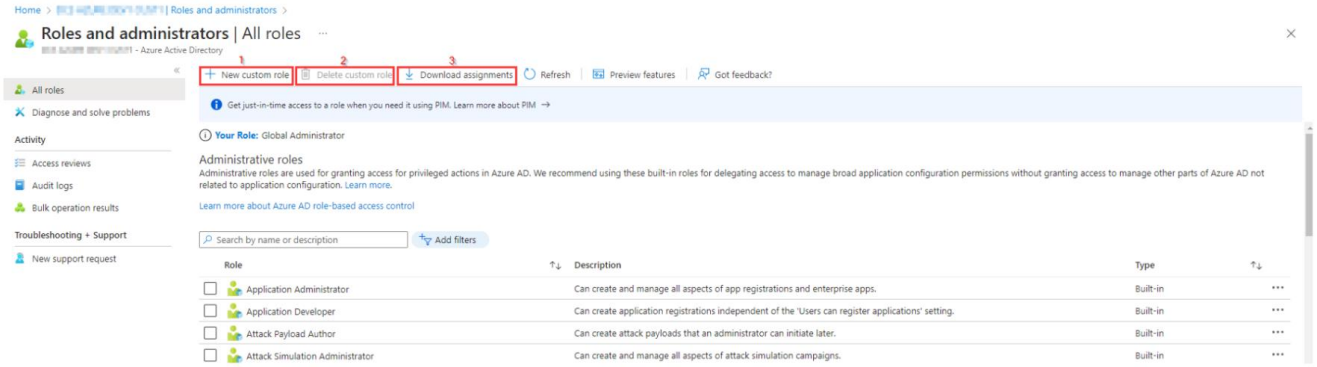
**Download groups [2]** is a good feature to create a report on all groups if there are a lot of groups created already. By selecting **Download groups** a windows is opened at the right top of the blade:




In this window the proposed file name can be changed and after **Start** is selected a csv will be created. If the creation of the csv file is succeeded, you will get the option to download the file.

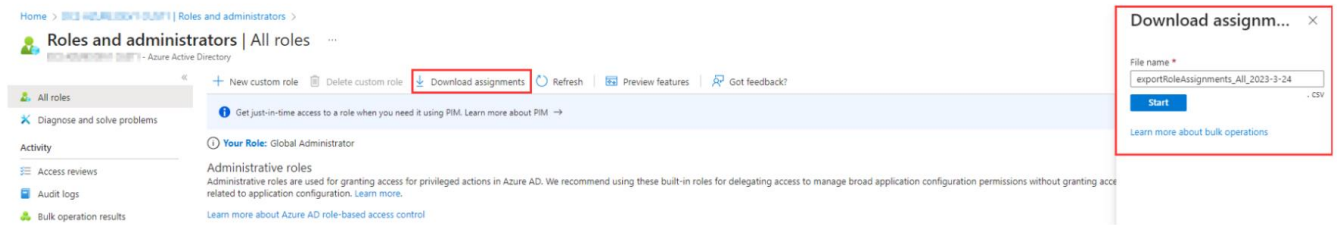
## 2.3 IAM Reports – Roles and Admins

The Roles and Admins tile in the dashboard redirects you to the Azure Active Directory Roles and Admins blade in the customer environment:




Administrative roles are used for granting access for privileged actions in Azure AD. In this blade you can create a **New custom role[1]**, **Delete a custom role [2]** or **Download assignments [3]**.

**Download assignments [3]** is a good feature to create a report on role assignments. By selecting **Download assignments** a windows is opened at the right top of the blade:



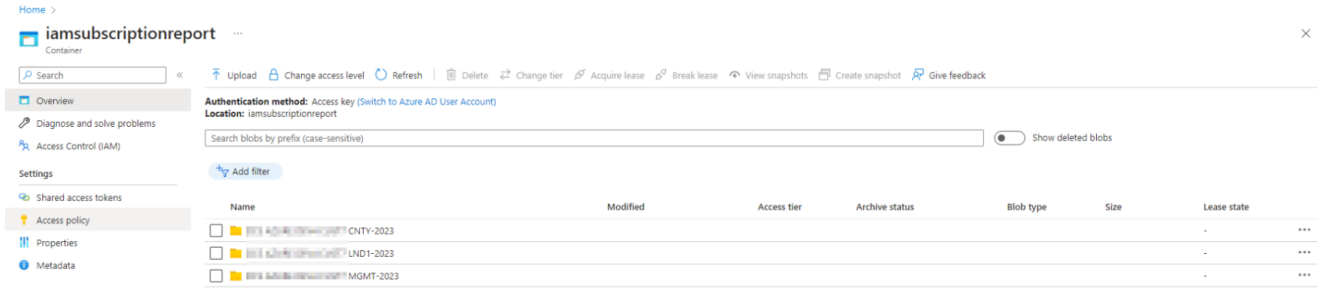
In this window the proposed file name can be changed and after **Start** is selected a csv will be created. If the creation of the csv file is succeeded you will get the option to download the file.

For more information about role-based access control check this link .

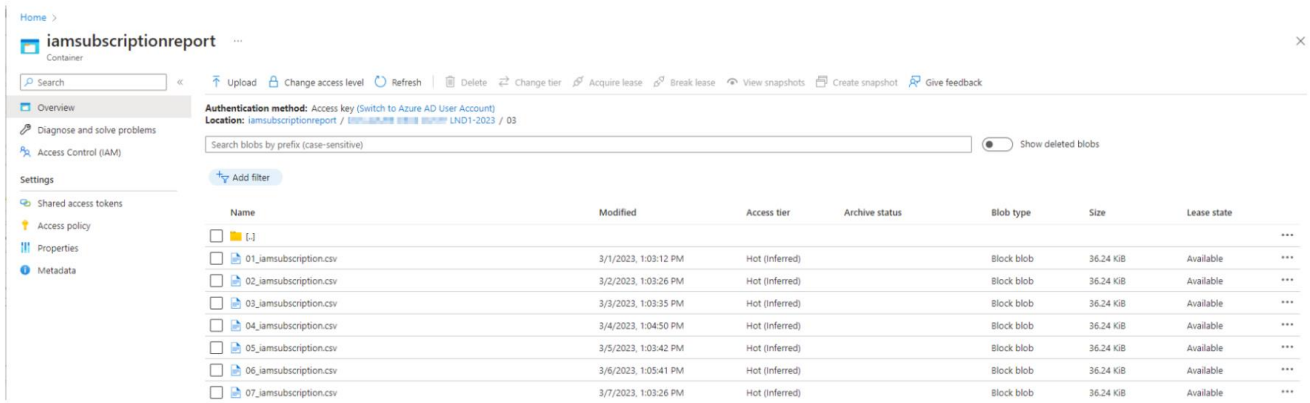
## 2.4 IAM Reports – Subscription Roles

The **Subscription Roles** tile redirects you to a **Storage container** where reports are saved that are created every 12 hours using the **Get-AzureSubscriptionRolesForReporting runbook**. For each day only one report is preserved.

The contents of this iamsubscriptionreport container will look like this.



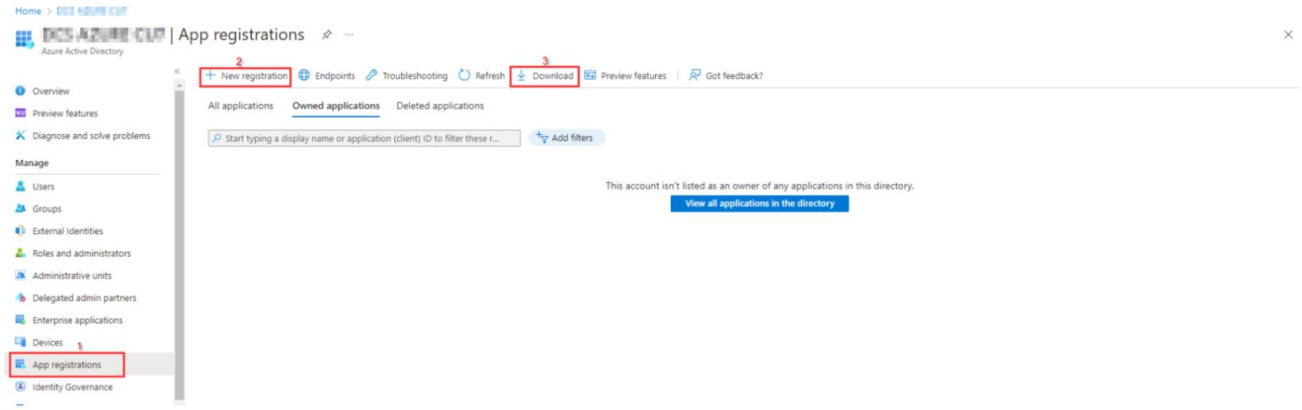

The **Subscription Roles reports** are reports that contains Subscription Role assignment information and are **created based on a schedule** and saved in **CSV file format**. The reports are saved **per subscription per year in a separate folder**. In every subscription folder you find folders with the numbers of the month. the contents of a monthly folder will look like this:




These reports can be used for monthly management reporting or for later reference.

## 2.5 IAM Reports – App Registrations

The App Registrations tile in the dashboard redirects you to the Azure Active Directory **App Registrations blade [1]** in the customer environment:

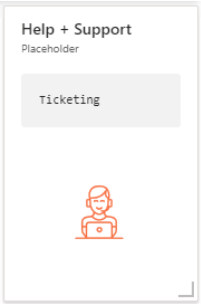



In this blade **New registrations [2]** for applications can be added to Azure Active Directory to establish a trust relationship between your application and the identity provider, the Microsoft identity platform. For more information about registering an application, check this link .

The **Download [3]** option enables you to create and download a CSV file with *All applications* or *Owned applications*.


Download app registrations
Select which app list you would like to download, and set the name for your new file. The download format for the app registrations will be based on the Microsoft Graph Application schema. Learn more
App list selection
All applications
Owned applications
File name
AppRegistrationList
.csv
Download

# 3. Help + Support




The Help + Support section has only one tile at this moment that is a placeholder that will redirect to the home blade of the Azure portal.

This section is meant to provide tile for Help and Support, like a tile to a ticketing service. As this is not available yet the Ticketing tile redirects to the Azure Portal.
In the future this link can be changed to redirect to a ticketing system or other means to provide help and support.

# 4. Operational Reports

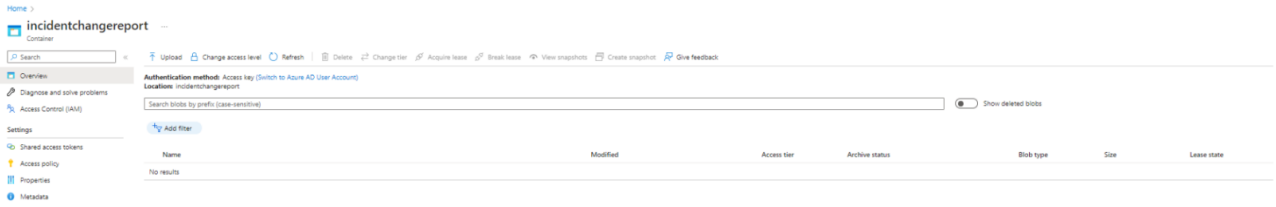

Operational Reports is a separate section in the dashboard that consists of 2 tiles that both contains a link to redirect you to a separate Storage Account container where the respective reports can be found:

Incident Report: Links to the incidentchangereport container at the storage account for reporting.

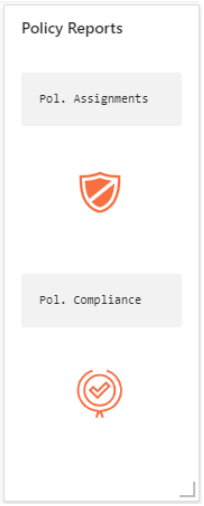
Change Report: Links to the incidentchangereport container at the storage account for reporting.

In the incidentchangereport container, where both links redirect to, reports, extracted from ITSM Service Now in PDF format should be manually uploaded once per month. The name should have a prefix of year-month-filename.

By default, this container will be empty:



# 5. Policies Reports




Policies Reports is a section in the dashboard that consists of 2 tiles that both contains a link to redirect you to a Azure blade where the respective reports can be found:

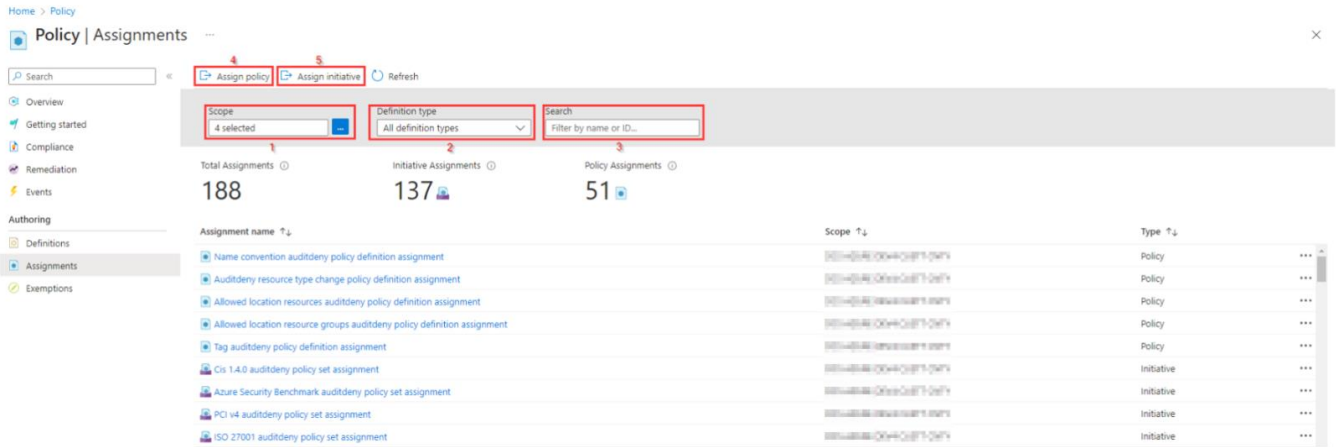
- Policy Assignments: Links to the Policy Assignments blade in Azure
- Policy Compliance: Links to the Policy Compliance blade in Azure

These reports provide details on active policies defined within the customer subscription(s). One of the largest benefits of Azure Policy is the insight and controls it provides over resources in a subscription or management group of subscriptions. For more information on Azure Policies, check this link .

## 5.1 Policy Assignments

The policy assignments blade in Azure provides an overview of all assigned policies and initiatives for the selected **Scope [1]**. By default all subscriptions are selected in the Scope filter, but it is possible to select one or more specific subscriptions to create an overview on.

With the **Definition type [2]** filter it is possible to select on '*Initiative*', '*Policy*' or on '*All definition types*'.




The **Search filter [3]** makes it possible to filter on a keyword are name in Initiative or Policy.

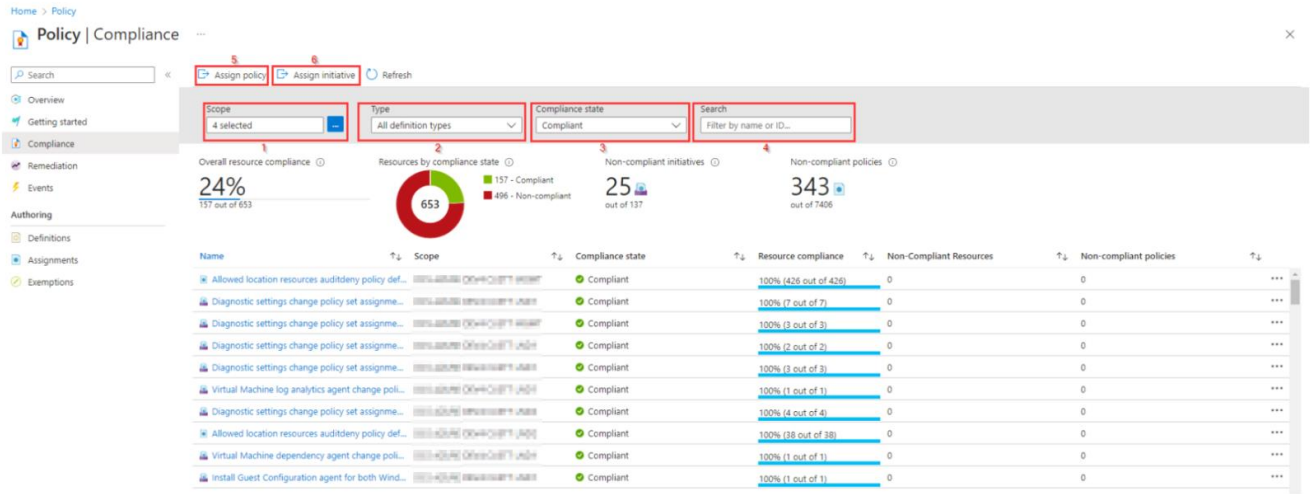
Apart from the overview it's also possible to **Assign policies [4]** or **Assign Initiatives [5]** in this Policy Assignments blade.

For more information about assigning policies, check this link .

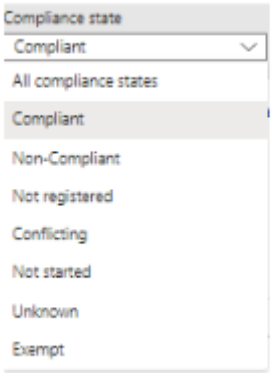
## 5.2 Policy Compliance report

The policy compliance blade in Azure provides an overview of the compliance state of policies and initiatives for the selected **Scope [1]**. By default all subscriptions are selected in the Scope filter, but it is possible to select one or more specific subscriptions to create an overview on.

With the **Type [2]** filter it is possible to select on '*Initiative*', '*Policy*' or on '*All definition types*'. The Compliance state filter [3]




The **Compliance state filter [3]** provides the option to filter on one of the following Compliance states:

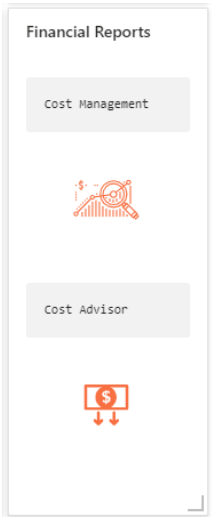


The **Search filter [4]** makes it possible to filter on a keyword are name in Initiative or Policy.

Apart from the overview it's also possible to **Assign policies [5]** or **Assign Initiatives [6]** in this Policy Assignments blade.

For more information about assigning policies, check this link .

# 6. Financial Reports



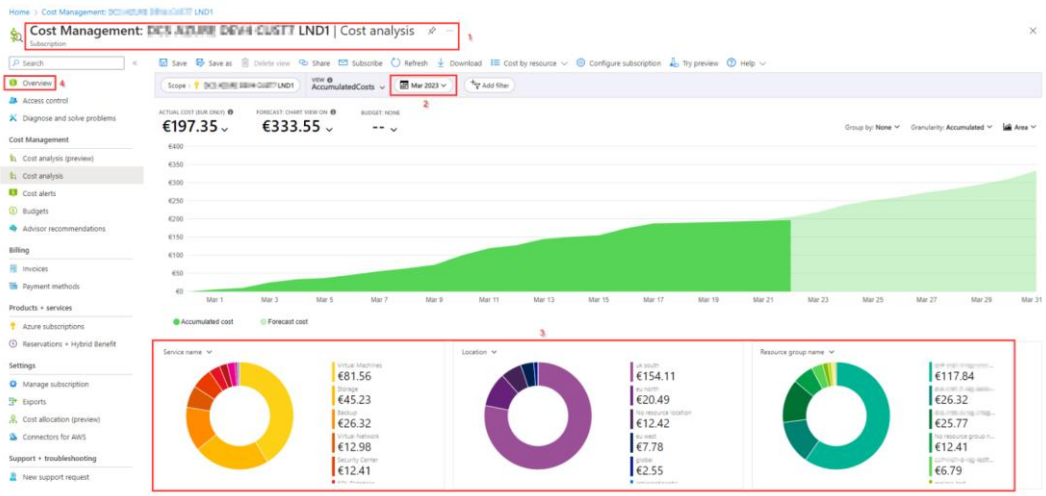

Financial reports is a separate section in the dashboard that consists of 2 tiles that both contains a link to redirect you to an Azure blade that contains information about:

- Cost Management: This tile redirects to the Cost Analysis blade in Azure Cost Management.
- Cost Advisor: This tile redirects to the Advisor recommendations blade in Azure Cost Management.

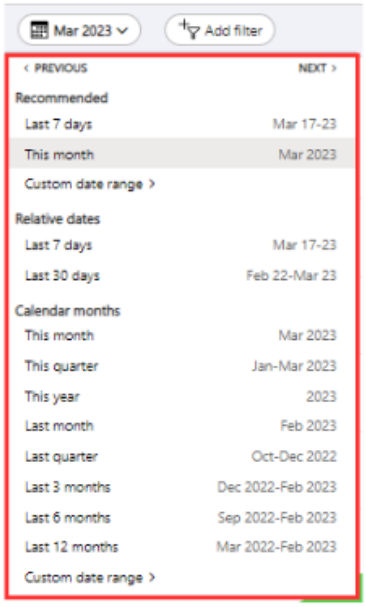
These reports provide details on the charges attracted by services in use in the customer subscription(s). To do cost analysis an Enterprise subscription is needed. With a CSP subscription cost analysis is not possible.

## 6.1 Cost Management

By selecting the Cost Management tile you are redirected to the following blade in Azure:



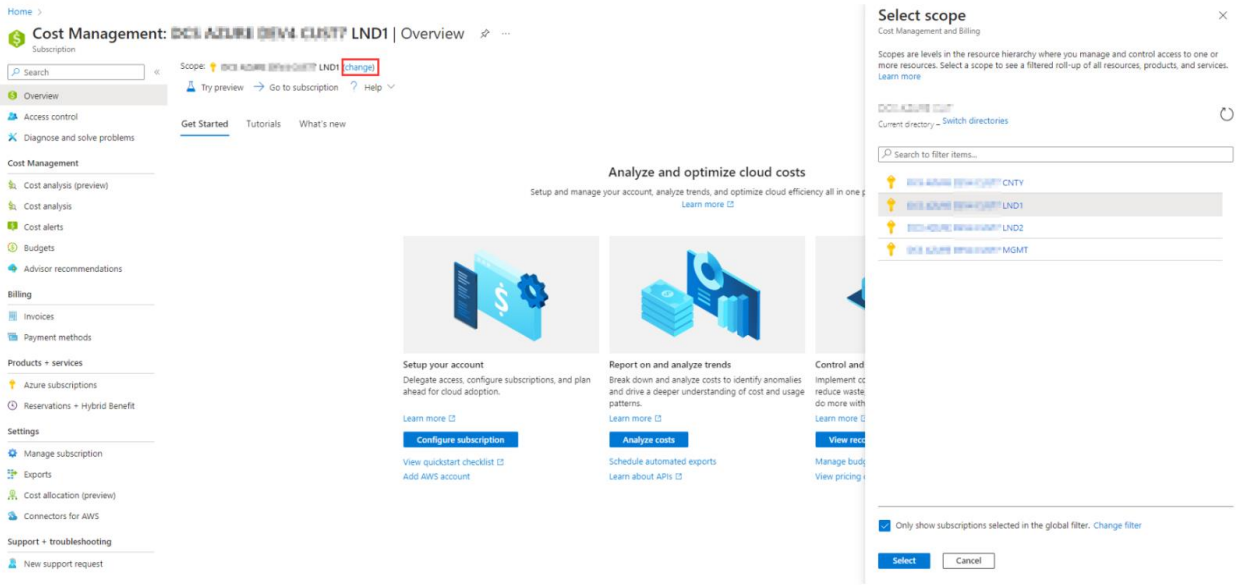

At the top of this **blade [1]** you find the subscription for which the Cost Management blade is visible.
Cost Management is visible on a per subscription overview. The overview provides the actual cost and a forecast for the selected **time range [2]** Possible time ranges are:




where **Custom date range** can be a range within the last 2 years.

At the bottom of the blade there are **3 pie charts [3]** with more detailed cost information on specific resources, services or tags that can be selected in the filters on top of the pie chart.

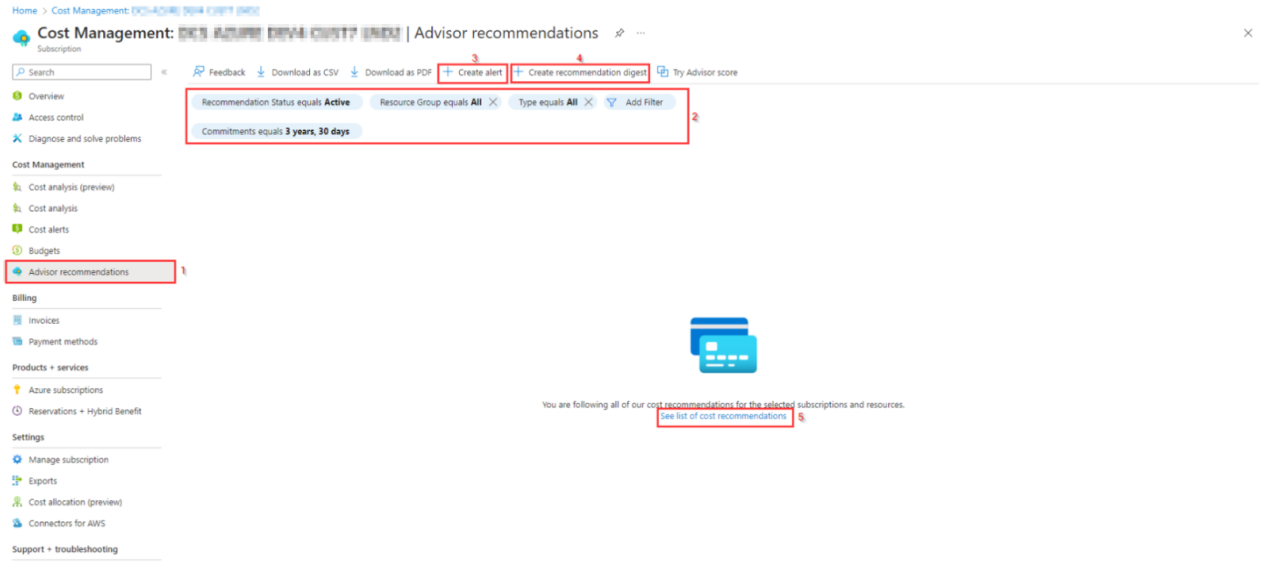
To change the scope for cost management, select **Overview [4]** at the left of this blade and click on **(change)** to select another subscription or a resource group within a subscription.




For more information about this Cost Management blade, check this link .

## 6.2 Cost Advisor

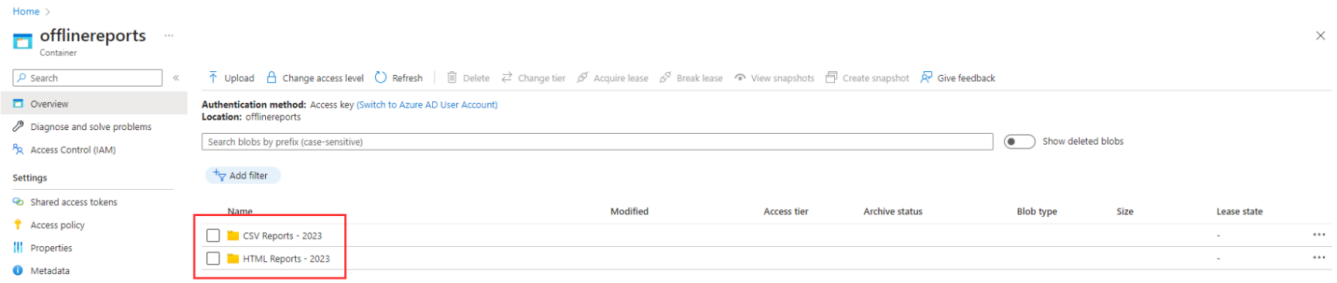
By selecting the Cost Advisor tile you are redirected to the **Advisor recommendations blade [1]** in Azure:




Based on the selection in the **filters [2]** at the top of this blade there are Advisor recommendations shown, if any.
In this blade it is possible to **Create alerts [3]** or **Create recommendation digests [4]**.
More information about **cost recommendations [5]** can be found by selecting this link

# 7. Offline Reports

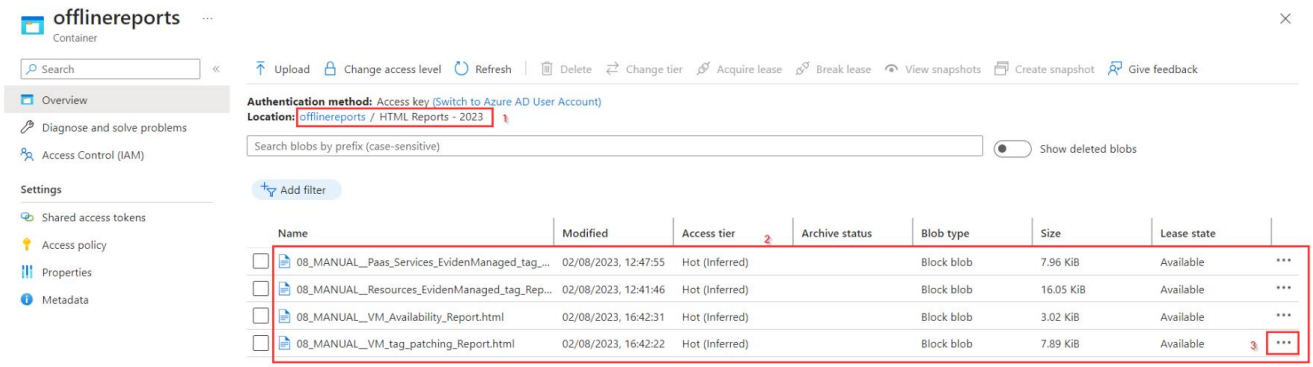
The Offline Reports tile redirects you to the **offlinereports** container where the offline reports are created in both CSV and HTML format, both in a separate folder for each year.




By default, the following reports can be found, that are created at the end of each month:

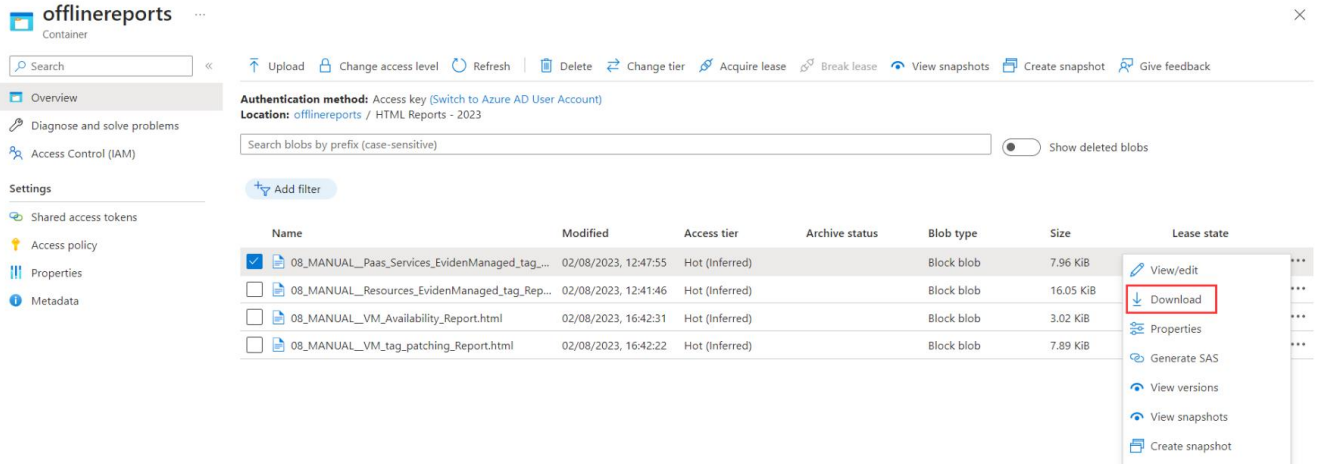
- **Resources with Eviden Managed tag**: provides an overview on a monthly basis with all resources that has the **EvidenManaged** tag set with value "*True*".
- **VM tag and patching**: provides an overview on a monthly basis with the patch settings and values for the Eviden tags.
- **VM availability**: provides an overview on a monthly basis with the availability of each VM.
- **PAAS services with EvidenManaged Tag**: provides an overview on a monthly basis with the PAAS Services that has the EvidenManaged tag set to '*True*'

The reports can be found by selecting the folder for the CSV or HTML, like for example **"HTML Report - 2023" [1]**:



In this folder for 2023 a report is created each month starting with the number of the **month [8]**. The text '*MANUAL*' between underscores after the number of the month means that the runbook that created the offline report is manually started. When the report is created by a schedule, as is usually the case for a monthly report, this text omits.

By selecting the **three-dots [3]** at the right of the file name a menu is opened where the file can be downloaded and opened (for an HTML file) or imported in excel (for a CSV):




The following reports will be available for download in both CSV and HTML format (where XX = # Month):

**Cloud Core reports**:

- *XX_Resources_EvidenManaged_tag_Report*: Overview of resources with EvidenManaged tag set to True.

**OS-management reports**:

- *XX_VM_tag_patching_Report*: Virtual Machine overview Eviden management Tags and Patching status.
- *XX_VM_Availability_Report*: Virtual Machine availability monthly overview.

**PAAS Services Management reports:**

- *XX_Paas_Services_EvidenManaged_tag_Report*: PAAS services with EvidenManaged tag set to True overview.

## 7.1 Overview of resources with EvidenManaged tag is True.

This offline report provides an overview of all resources in the customer environment that has the Eviden Managed tag set to True.

In HTML the report will look like this:

**Resources with EvidenManaged tag is "true" monthly Report 2023/08**

| RESOURCE NAME | TYPE | SUBSCRIPTION | RESOURCE GROUP |
|---|---|---|---|
| 0c60cb2f-f15e-5e70-94f4-14e02079e21b | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 15e69b12-3ac0-508d-b019-8bc5a9520780 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 2333675c-d0c5-5ccc-9f7e-9aad4b9edb4c | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 2ed365f1-90de-5414-9f02-8bc499255123 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 32d8bcb4-b953-5fe6-bd18-6f0a2f025883 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 35cf9b8c-0d28-5ebd-99a6-1c436bd16ba8 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 36e78b63-ed19-5ade-957f-c73436943484 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 4180b998-4a2f-54ff-afbb-0006a85c97a8 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 43e1dff3-6814-523f-9d28-cedbf6a8c3a0 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 4e37c44c-477d-5b81-964e-1bd954417a31 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 546ed212-ee4a-5b5a-8f33-25d08c250ae2 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 58feb3ed-02b4-58c7-8250-08b802445319 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 5935553c-3279-57d8-8d2c-8d2ef020ae9c | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 5cd07614-bfef-50f1-80ff-1a5fd03a5049 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 686618ba-9479-574b-a0a2-e4acb272f662 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 6ffd986a-774d-5086-8547-e348f26caab5 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 75b08639-dba6-5888-a34e-4aeffbf720fa | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 7c4a98e9-d92f-5453-960f-b32ede31320b | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 847edb8f-9151-5157-85b3-95e5dfc5b715 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 8fde7685-2a57-53a2-bfe9-36ac845be275 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 9039b0db-3c3a-516d-a0df-c52bc3e54b80 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |
| 98d00e5b-54bd-5908-b0e7-48f2a3982a29 | microsoft.insights/workbooks | [redacted] MGMT | [redacted] |

**Known Issue's**

If the query doesn't find any resource (No resources with EvidenManaged tag set to True are available in customer environment) only the title of the report and a message (in red) is shown in the HTML report. The CSV report will be empty.

## 7.2 Virtual Machine overview Eviden management Tags and Patching status

This offline report provides an overview of Virtual Machines in the customer environment and the tags that are used for Eviden Management. This report also provides and overview if the virtual machine is patched.

In HTML the report will look like this:

**VM Tagging and Patching monthly Report 2023/08**

| VIRTUAL MACHINE | RESOURCE GROUP | SUBSCRIPTION | PATCHSTATE | EVIDENPATCHING | EVIDENOSVERSION | EVIDENMANAGED | EVIDENANTIMALWARE | EVIDENCOMPLIANCE | EVIDENBACKUP | EVIDENENCRYPTION |
|---|---|---|---|---|---|---|---|---|---|---|
| alkeshvmfordevelop | [redacted] | [redacted] LND1 | VM does not have the correct tags | | | False | False | False | | False |
| linvm01 | [redacted] | [redacted] LND2 | VM is EvidenManaged but not in Patch Schedule | Linux-Dev | | True | False | False | | False |
| linvm02 | [redacted] | [redacted] LND2 | VM is EvidenManaged but not in Patch Schedule | Linux-Test | | True | False | False | | False |
| linvm03 | [redacted] | [redacted] LND1 | VM is EvidenManaged and in Patch Schedule | Linux-Dev | redhat 8.7 | True | False | False | Gold | False |
| snowpocfred001 | [redacted] | [redacted] LND1 | VM does not have the correct tags | | | False | False | False | | False |
| winvm01 | [redacted] | [redacted] LND1 | VM is not EvidenManaged but is in Patch Schedule | windows-dev | | False | False | False | Silver | False |
| winvm03 | [redacted] | [redacted] LND2 | VM is EvidenManaged but not in Patch Schedule | windows-dev | | True | False | False | Gold | False |
| winvm06 | [redacted] | [redacted] LND1 | VM is EvidenManaged and in Patch Schedule | windows-dev | Windows Server 2016 Datacenter | True | False | False | | False |
| winvms07 | [redacted] | [redacted] LND1 | VM does not have the correct tags | | | False | False | False | | False |

### Known Issue's

If the query doesn't find any resource (No VM's are available in customer environment) only the title of the report and a message (in red) is shown in the HTML report. The CSV report will be empty.

## 7.3 Virtual Machine availability monthly overview

This offline report provides an overview of Virtual Machines in the customer environment with their availability over a month and if the virtual machine is managed by Eviden.

In HTML the report will look like this:

**VM availability monthly Report 2023/08 for log analytics workspace: [redacted]-mgmt-t-loganalytics**

| VIRTUAL MACHINE | OPERATING SYSTEM | SUBSCRIPTION | RESOURCE GROUP | START TIME RANGE | END TIME RANGE | AVAILABILITY PERCENTAGE | TOTAL AVAILABLE HOURS | TOTAL HOURS | MANAGED BY EVIDEN |
|---|---|---|---|---|---|---|---|---|---|
| testfredaks01 | Linux | [redacted] LND1 | [redacted] | 23-08-01 [00:00:00] | 23-08-01 [00:00:00] | 45.0 % | 18 | 40 | VM testfredaks01 is deleted before end of the month |

### Known Issue's

If a virtual machine is created within the reported month this is not mentioned in the report, but availability percentage during the month will be less then 100%.
If the query doesn't find any resource (No VM's are available in customer environment) only the title of the report and a message (in red) is shown in the HTML report. The CSV report will be empty.

## 7.4 PAAS services with EvidenManaged tag is True.

This offline report provides an overview of all PAAS Services in the customer environment with the status of the Eviden Managed tag.

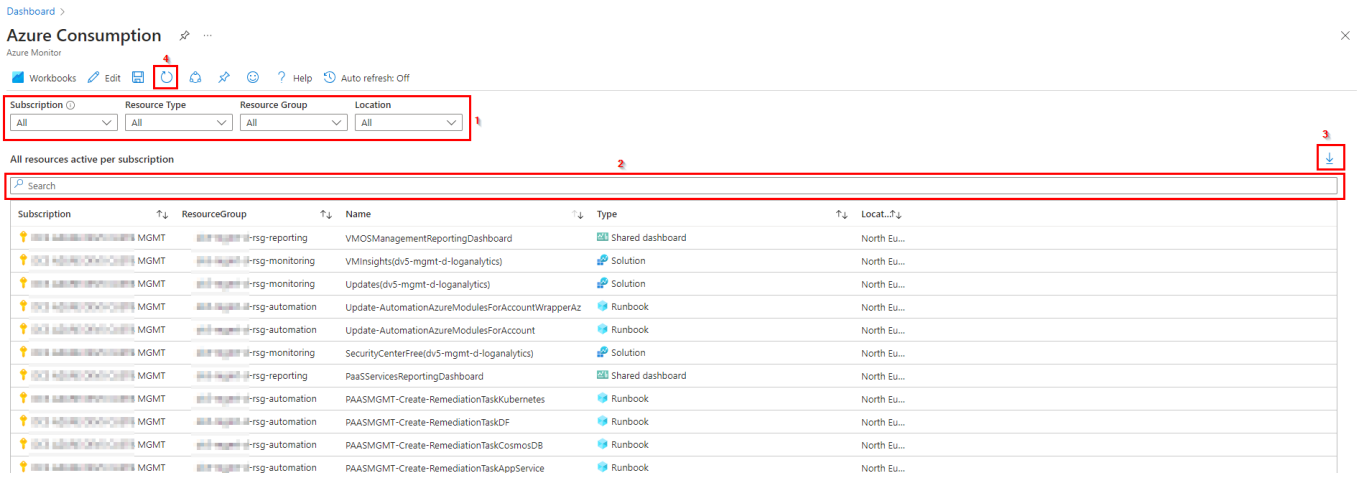
In HTML the report will look like this:

# PAAS Service overview with EvidenManaged State monthly Report 2023/08

| NAME | TYPE | RESOURCE GROUP | SUBSCRIPTION | LOCATION | EVIDEN MANAGED |
|---|---|---|---|---|---|
| dv4-mgmt-t-logicapp-itsm-alerts | microsoft.logic/workflows | [redacted] | [redacted] MGMT | uksouth | False |
| Daily_atsix_start | microsoft.logic/workflows | [redacted] | [redacted] LND1 | westeurope | False |
| Daily_atnine_stop | microsoft.logic/workflows | [redacted] | [redacted] LND1 | westeurope | False |
| ststv2_vms_AutoStop | microsoft.logic/workflows | [redacted] | [redacted] LND1 | westeurope | False |
| testcheck | microsoft.logic/workflows | [redacted] | [redacted] LND1 | westeurope | False |
| ststv2_vms_Sequenced_start | microsoft.logic/workflows | [redacted] | [redacted] LND1 | westeurope | False |
| ststv2_vms_Scheduled_start | microsoft.logic/workflows | [redacted] | [redacted] LND1 | westeurope | False |
| ststv2_vms_Sequenced_stop | microsoft.logic/workflows | [redacted] | [redacted] LND1 | westeurope | False |
| ststv2_vms_Scheduled_stop | microsoft.logic/workflows | [redacted] | [redacted] LND1 | westeurope | False |
| dv4-mgmt-t-logicapp-itsm-cmdb | microsoft.logic/workflows | [redacted] | [redacted] MGMT | uksouth | False |
| bbd-hrut-d-functionapp-billing | microsoft.web/sites | [redacted] | [redacted] MGMT | westeurope | False |
| dv4-mgmt-t-functionapp-ostagging | microsoft.web/sites | [redacted] | [redacted] MGMT | uksouth | False |
| dv4-mgmt-t-functionapp-billing | microsoft.web/sites | [redacted] | [redacted] MGMT | uksouth | False |
| startstopv2testcheck | microsoft.web/sites | [redacted] | [redacted] LND1 | westeurope | False |
| dv4-mgmt-t-functionapp-itsm-pwsh | microsoft.web/sites | [redacted] | [redacted] MGMT | uksouth | False |
| startstoppocama347xe4b42w | microsoft.web/sites | [redacted] | [redacted] LND1 | westeurope | False |

# 8. Azure Consumption workbook

The Azure Consumption report is used to provide an overview of all Azure services in use in customer subscription(s) managed by Eviden.




In the top part the report provides several **filters [1]** to select the resources to report on for a specific Subscription, Resource Type, Resource Group or Location. This way the filters at the top of the report can be used to get a clear overview on specific subscription, resource groups, resource types or locations.

To search for a specific resource or resources containing a specific name, the **search bar [2]** above the columns can be used. The selected resources based on the **filters [1]** and/or the text in the **search bar [2]** can be **Exported to Excel** with the **Export button [3]** at the right top of the overview.

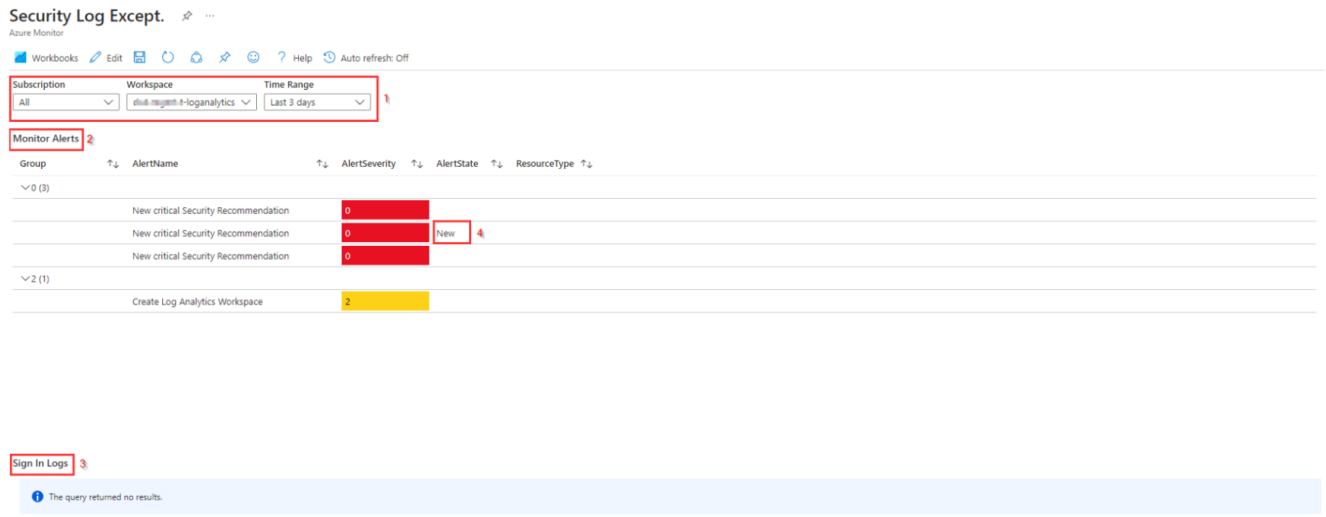
At the top of the report the **refresh button [4]** is available to refresh the overview.

# 9. Security Log Exception workbook

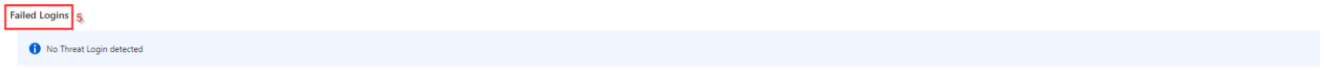
The Security Log Exception Report is a basic report that shows in brief the security log exceptions from the selected log analytics workspace, in 4 separate overviews:

- Monitor Alerts
- Sign In Logs
- Failed Logins
- Security Alerts

On top of this report there are **filters [1]** to select the Subscription (for the log analytics workspace), Workspace and the Time Range.
Based on the selected log analytics workspace(s) and time range the overview for **Monitor Alerts [2]** and **Sign In Logs [3]** will look like this:




In the Monitor Alert part, if an Alert is raised in the past 24 hours **New [4]** is added to the AlertState Column.
In the bottom part of this report **Failed Logins [5]** and **Security Alerts [6]** are shown, if any.


Failed Logins
No Threat Login detected

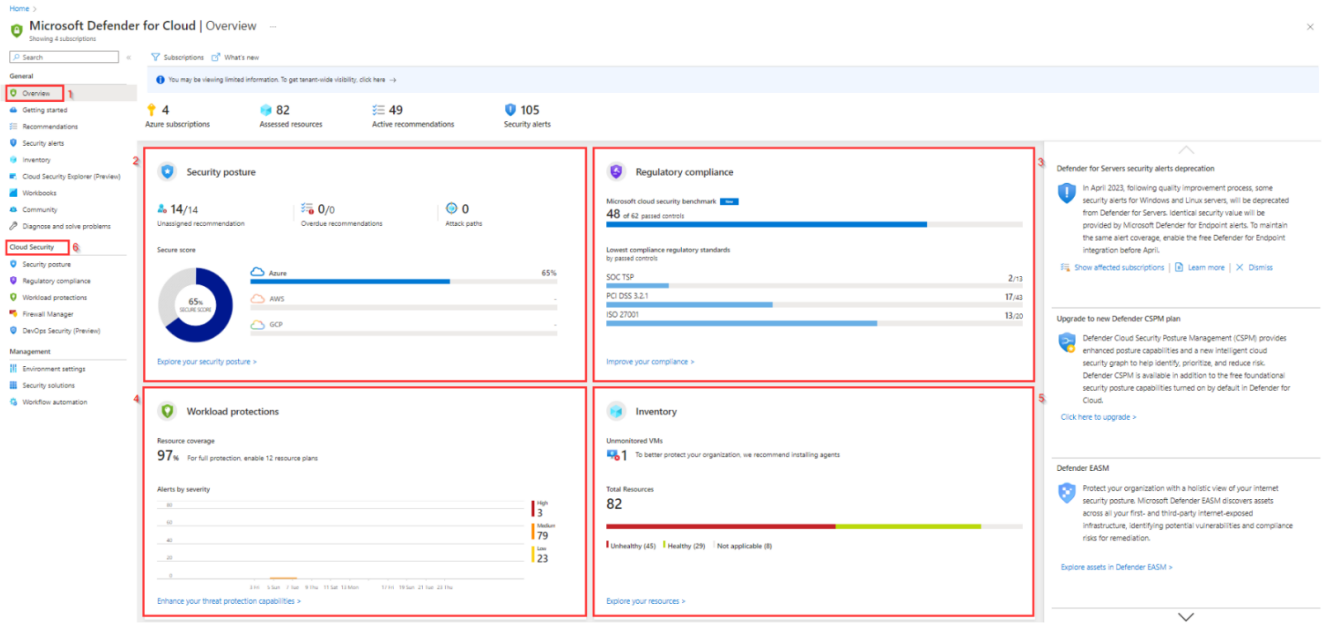

Security Alerts
The query returned no results.

# 10. Compliance report

The Compliancy Report tile redirects you to the Microsoft Defender for Cloud Overview blade in Azure.
Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. For more information about Microsoft Defender for Cloud, check this link .

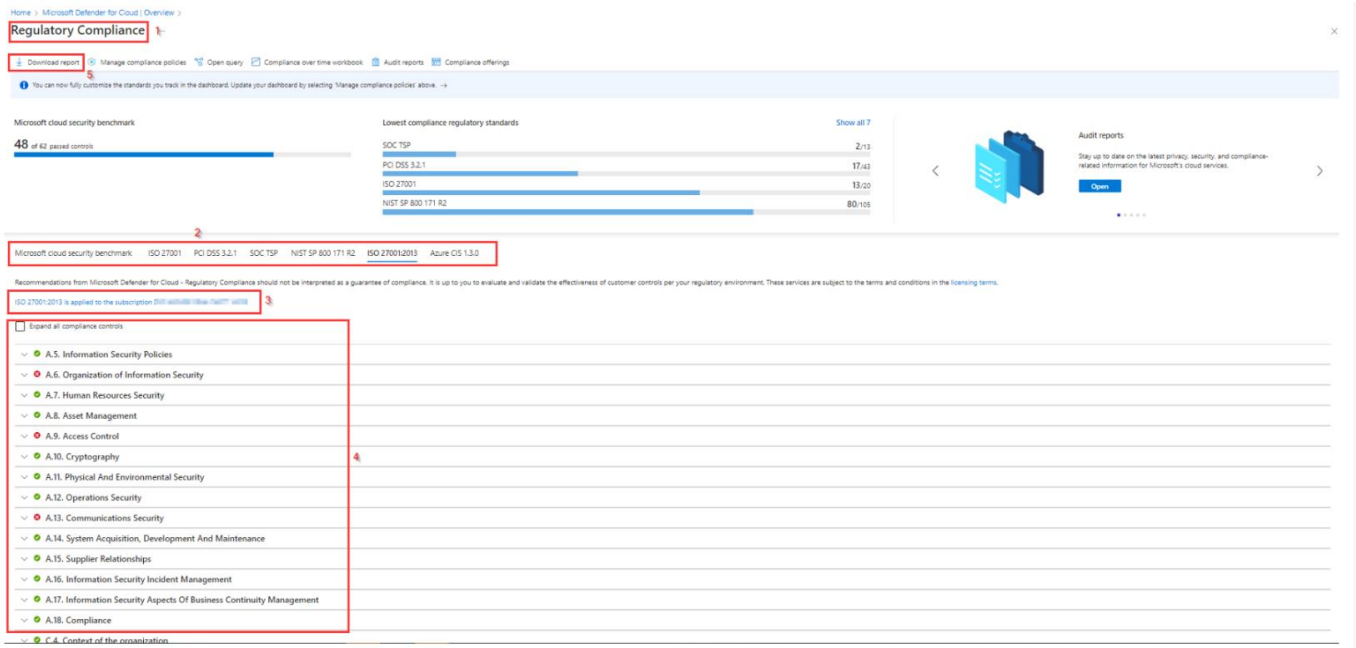
In the **overview blade [1]** of Microsoft Defender for Cloud there are 4 tiles with more detailed Cloud Security information:

- **Security Posture [2]**
- **Regulatory compliance [3]**
- **Workload protections [4]**
- **Inventory [5]**




For Security Posture, Regulatory compliance and Workload protections it is also possible to open this information in a separate blade by selecting the respective blade under **Cloud Security [6]**

By selecting the **Regulatory compliance** tile a separate blade for Regulatory Compliance [1] is opened and shows **compliance standards [2]** that are represented in Defender for Cloud's regulatory compliance dashboard. Each standard is an initiative defined in Azure Policy.




For the **selected benchmark [3]** is shown to which subscription the benchmark is applied and an expandable **overview [4]** of the compliance controls is shown.

The compliance report with the results for the selected benchmark can also be downloaded as a PDF or CSV by selecting the **Download report [5]** option on top of this blade.

For more information about the regulatory compliance and the standards that are available in Defender for Cloud check this link

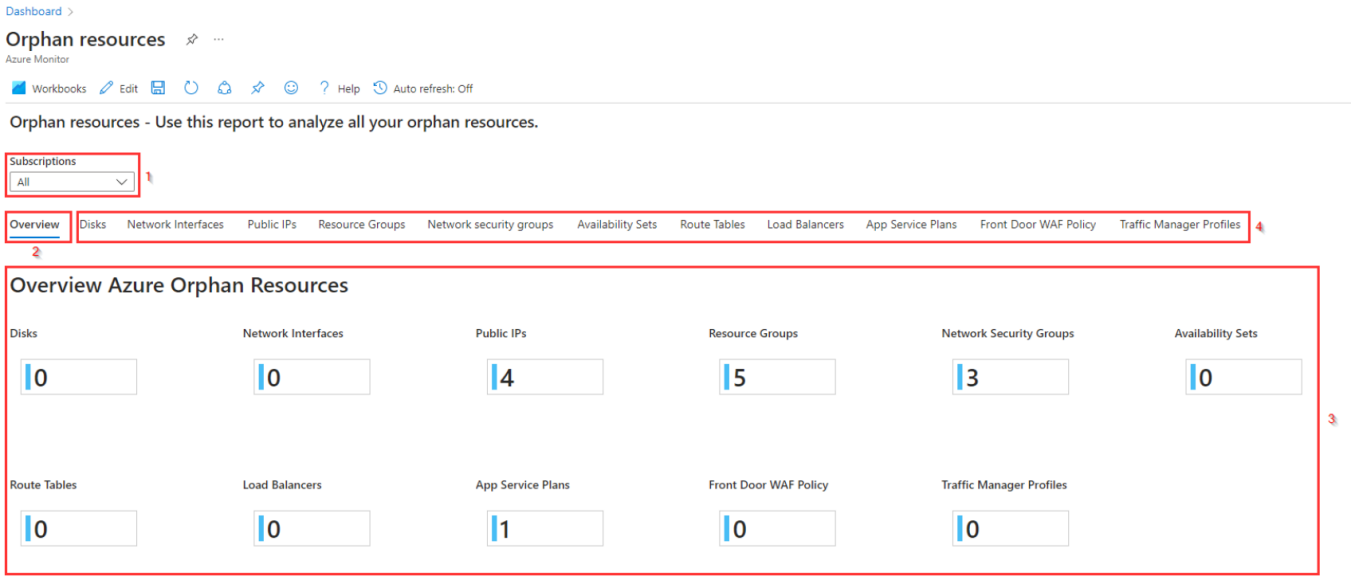
# 11. Orphan resources workbook

The Orphan Resources report is used to make the orphaned resources per resource type visible. The report has 2 parts:

- The orphaned resource overview blade
- A detailed blade per orphaned resource type

## 11.1 The orphaned resource overview blade

In the top part it is possible to **filter [1]** on Subscription.
When the report is opened by default an **overview [2]** of all possible orphaned resources is displayed together with the number of **orphaned resources [3]** found per type.




Next to the overview blade you will find a more detailed overview with a **separate blade per orphaned resource type [4]** that at this moment is added to this report, like:

- Disks
- Network Interfaces
- Public IPs
- Resource Groups
- Network security groups
- Availability Sets
- Route Tables

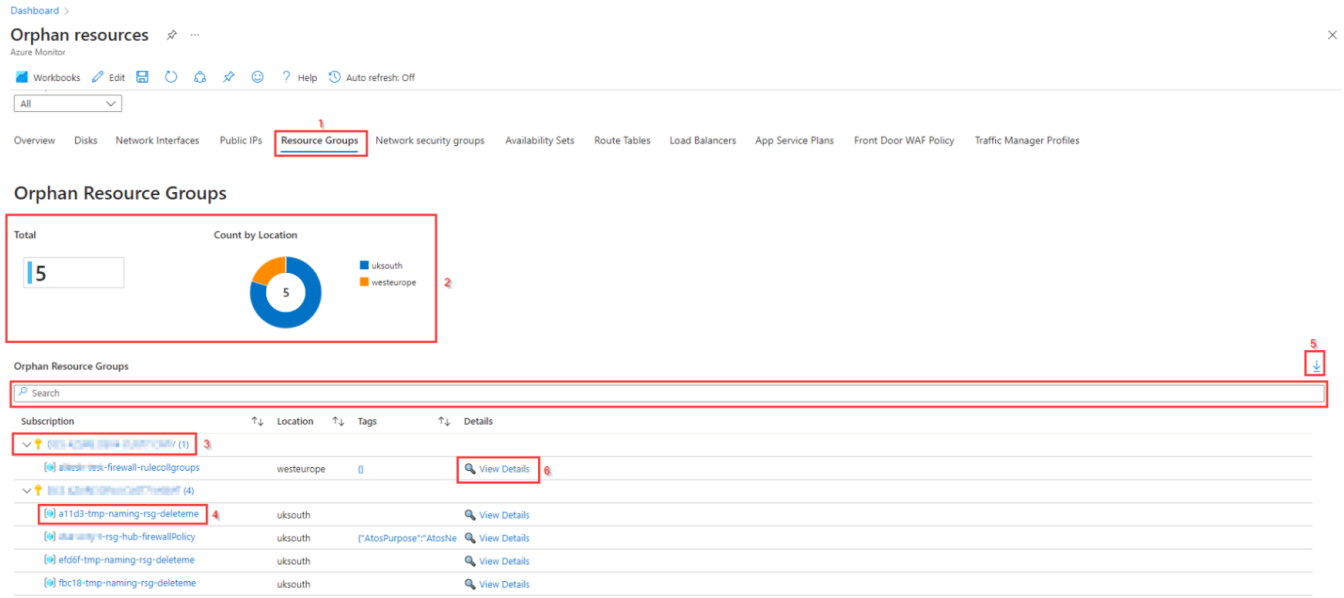
- Load Balancers
- App Service Plans
- Front Door WAF Policy
- Traffic Manager Profiles

For more detail about a specific orphaned resource type, you can select the blade for the resource type.

## 11.2 A detailed blade per orphaned resource type

The overview blade only shows the number of orphaned resources per resource type that possible can contain orphaned resources.

If there are orphaned resources you can select the **blade [1]** for the specific type of resource to show more detailed information about the resource, like in the above picture for the orphaned resource groups:



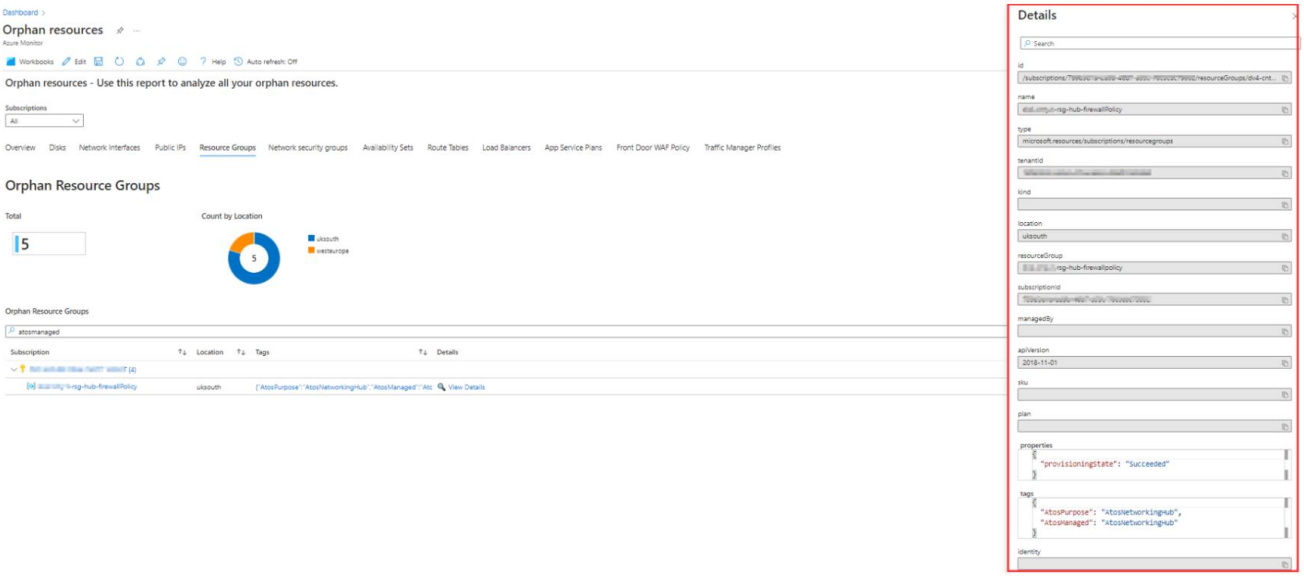

As shown in this blade the **total number of orphaned resource groups together with the count per location [2]** is visible at the top of this blade. In the bottom part you find an overview of the orphaned resource groups **grouped by subscription [3]**.

In this blade it is also possible to select the **name of the resource [4]** to be redirected to the resource it selves, where the orphaned resource can be deleted if needed.

Above the columns is a **searchbar [5]** to search for a specific **resource**, **location** or resource with a specific **tag**.

At the right side of the resource type blade, you find the **export option [5]** that can be used to download a csv with all resources of this type.

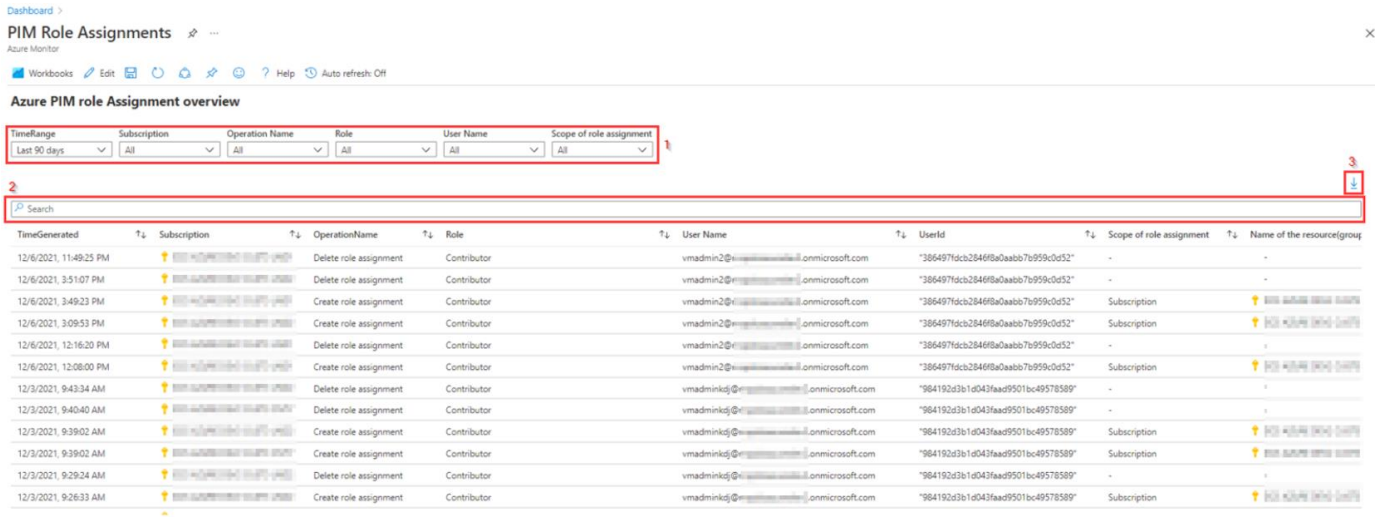
By selecting **View Details [6]** an overview section with more detail about the resource (group) is shown.



# 12. PIM Role Assignments workbook

The PIM Role Assignments report is used to make the assignments of privileged role for a selected time period visible in an overview.

In the top part the report provides several **filters [1]** to select the **Time Range** and to filter on **Subscription**, **Operation Name** (create or delete), **Role** that is assigned or revoked, **UserName** and **Scope of role assignment** (Subscription, Resource Group, Resource or None (-)).




Underneath the filters there is a **search bar [2]** available for more specific filtering like searching on a specific resource.

The report it selves shows the creation and deletion of role assignments in the following columns:

- **TimeGenerated**: time when creation or deletion of role occurred.
- **Subscription**: Subscription in which the role is assigned
- **OperationName**: Shows the operation, if the role was assigned or deleted from the User account.
- **Role**: name of the role that was assigned
- **UserName**: Name of the user account that got the role assigned. In most cases this shows the e-mail address of the user if it can be found as this information is only available in the log if the user performed any action in Azure during the selected time range.
- **UserId**: Id of the user account that got the role assigned. This information is always available in the log and can be used (if needed) to determine the username.

- **Scope of role assignment**: A role can be assigned to a **Subscription**, **Resource group** or even to a specific **Resource**. In this column the scope is visible for role assignments. When a role is deleted a dash (-) is visible.
- **Name of the resource(group)**: If a role is assigned, this column show to which **Subscription**, **Resource group** or **Resource** the role is assigned. When a role is deleted a dash (-) is visible.

For the creation of a csv based on the report that is visible, the **download option [5]** at the **right top** above the search bar is available.

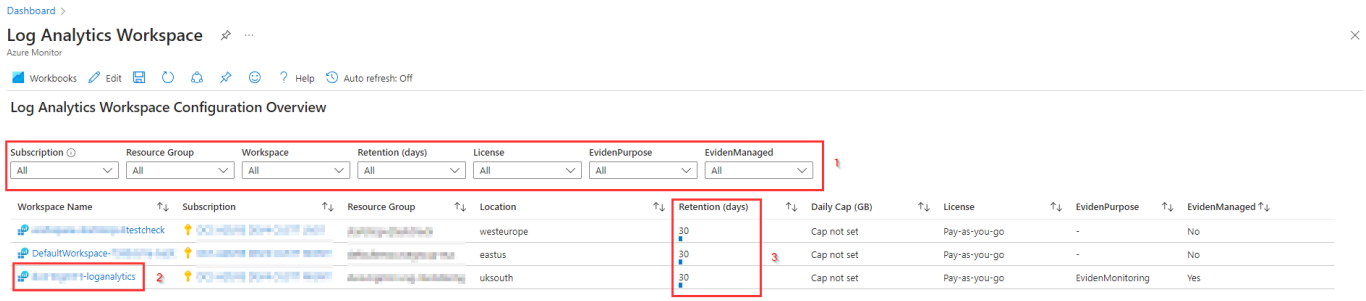
# 13. Log Analytics Workspace workbook

The Log analytics Workspace report consists of 2 parts:

- **Log Analytics Workspace Configuration Overview**: Provides an overview of the Azure Log analytics Workspaces and their configuration that are created in the Azure environment.
- **Log Analytics Workspace Workloads**: An overview of the Log analytics Workspaces with operational data divided in 3 blades:
    - **Health Overview**: Provides an overview of the health of all log analytics workspaces.
    - **Usage Overview**: Graphical overview of the log usage for a selected log analytics workspace and a selected time range.
    - **Detailed Usage**: A detailed overview of the table usage for a selected log analytics workspace and a selected time range.

## 13.1 Log Analytics Workspace Configuration Overview

In the top part it is possible to **filter [1]** on Subscription, Resource Group, Workspace, Retention, Licence, EvidenPurpose tag and if the Log Analytics Workspace is managed by Eviden.




The report shows an **overview of the Log Analytics Workspaces** that are created with their configuration like **Retention, Daily Cap, Licence, EvidenPurpose** tag and if the **EvidenManaged** tag is set to **Yes**.

For more detail about a Log Analytics Workspace is is possible to select the name of the **Log Analytics Workspace [2]** to open the **Log Analytics Workspace blade**.

In the column **Retention (days) [3]** you will find the retention together with a small graphical view on the number of days for the retention.

## 13.2 Log Analytics Workspace Workloads

The bottom part of the Log Analytics Workspace report provides workload data based on Azure Health and the Azure Logs for Log Analytics Workspace.

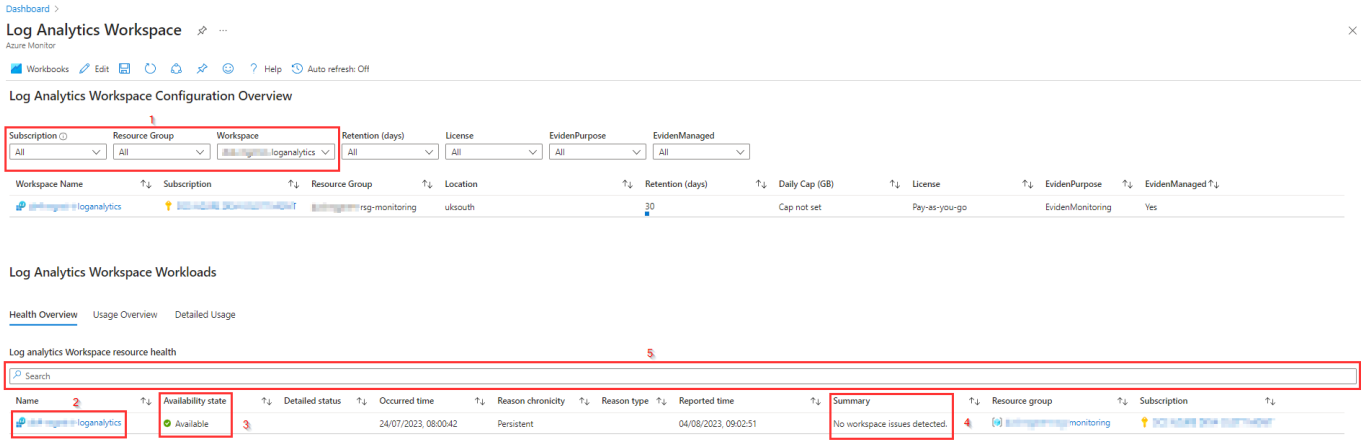
The Log Analytics Workspace Workloads reporting part consists of 3 blades:

- Health Overview
- Usage Overview
- Detailed Usage

Below the blades are described in more detail

### 13.2.1 Health Overview

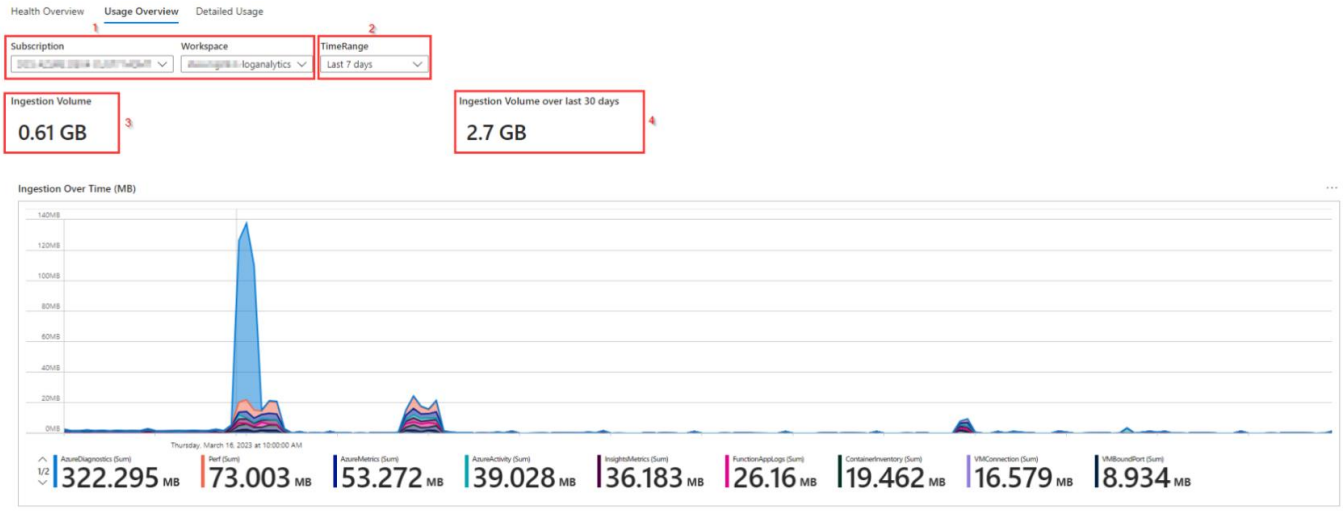
For the selected **Subscription(s), Resource Group(s)** and **Workspace(s)** in the **filter [1]** at the top of the report this blade shows an overview with the **health status** of the Log Analytics Workspace(s).
It shows the **Availability State [2]**, **Detailed Status** (if available), the data and time the workspace changed to this state (**Occurred Time**), if the status is Persistent or Transient (**Reason Chronicity**), the **Reason type** and a Summary [3] of the health state. The Summary [3] column adds some more detail in case the log analytics workspace doesn't show *Available* in the **Availability state [2]** column.




For more detail about a Log Analytics Workspace is is possible to select the **name of the Log Analytics Workspace [4]** to open the **Log Analytics Workspace** blade.
The **searchbar [5]** can be used to search for specific log analytics workspaces.

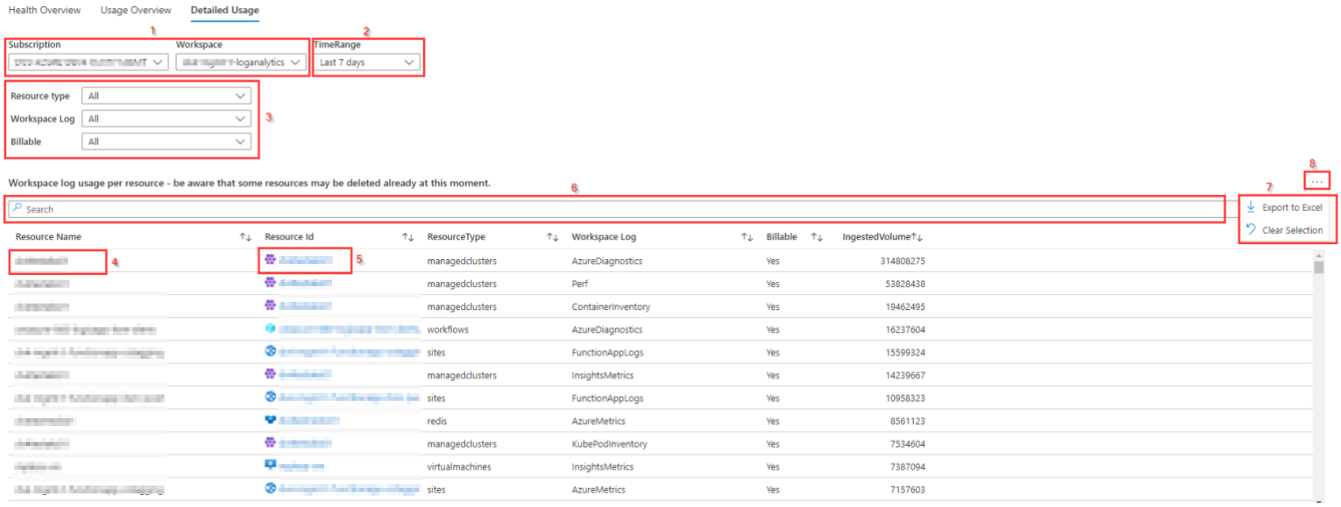
### 13.2.2 Usage Overview

The Usage Overview provides an overview of the ingestion data volume of a selected Log Analytics Workspace for a selected TimeRange.
The log Analytics workspace can be selected using **the Subscription and the Workspace filter [1]** while the desired time range can be selected using the **TimeRange filter [2].**




On the top of the overview the total **ingested Volume [3]** is shown, based on the selected Time Range (at the left) and the **ingested volume over the last 30 days [4]**.

At the bottom, a graphical overview is shown with the **Ingestion Over Time** for the logs that are on the selected Log Analytics Workspace.




Be ware that the Ingested Volume is based on the selected time range. Based on this it is possible that the resource that is reported is already deleted at the time the report is created. This is also why the name in the **Resource Name [4]** column

is not shown as a link, but instead a separate column has been added with the **Resource Id [5]** that is shown as a link.
In case the resource is already deleted the Resource Id column will sometimes be empty. If the resource is shown as a link, it is still possible that you get an error page when selecting the link.

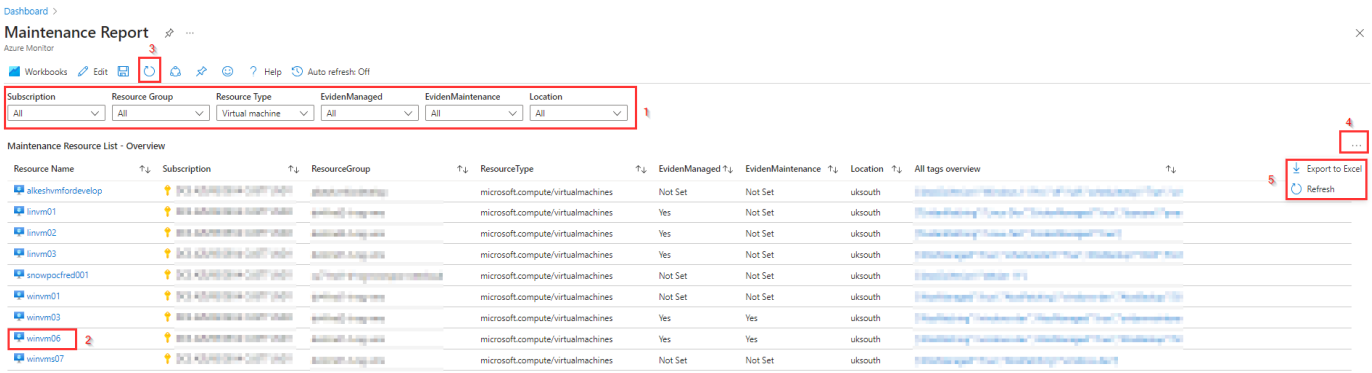
Use **Billable filter (set to Yes) [3]** to filter out logs that are most used by Azure it selves, like the Azure Activity log or use the **Workspace Log [3]** filter to select a specific log table at the log analytics workspace.
The **searchbar[6]** can be used to search for a specific resource.

You can use the **Export to Excel option [7]** to download the overview to a comma-separated file by first selecting the **three-dots [8]** at the right top of this blade.

# 14. Maintenance workbook

The Maintenance report provides an overview to show if the **EvidenManaged** and **EvidenMaintenance** tags are set to indicate that a resource is Eviden managed and in maintenance If the resource is in maintenance by setting the **EvidenMaintenance** tag to '*True*', no tickets are raised for this resource in case of an alert.

In the top part the report provides several **filters [1]** to select the Subscription, Resource group, Resource type, EvidenManaged tag, EvidenMaintenance tag and Location to report on. This way the filters at the top of the report can be used to get a clear overview of specific resources and EvidenManaged and EvidenMaintenance tag settings.




To change the value of a tag or define a tag, you can click on the **Resource Name [2]** in the report as this opens the blade for the selected Resource and make the changed in the **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 [3]** to get the new value displayed in the report.
When you select the **three-dots [4]** in the right top you find the **Export to Excel and the refresh option [5]**

# 15. Virtual WAN workbook

The Virtual WAN report is used to provide an overview of the Virtual WAN(s) deployed in the Azure environment together with all Virtual WAN related resources.

The report consists of several blades, starting with an overview followed with more detail for each resource that is part of the virtual WAN solution:

- **Overview blade**: Overview of deployed Virtual WAN solutions with configuration information, configured hubs and hub virtual network connection.
- **VPN Gateways blade**: Overview of VPN Gateways with hub connected to and configuration.
- **VPN Sites blade**: Overview of Virtual WAN VPN Sites with configuration, VPN Site links and status of the VPN Site links.
- **ExpressRoute Gateways blade**: Overview of ExpressRoute Gateways with configuration and ExpressRoute connections.

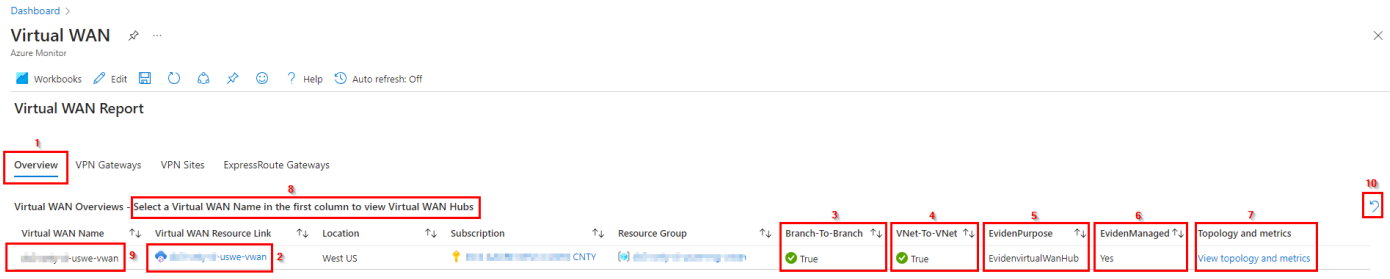
Below each blade is described in more detail

## 15.1 Overview blade

The **Overview** blade consists of three parts:

- Virtual WAN Overviews
- Virtual WAN Hubs
- Virtual WAN – Hubs – Connections/Peering

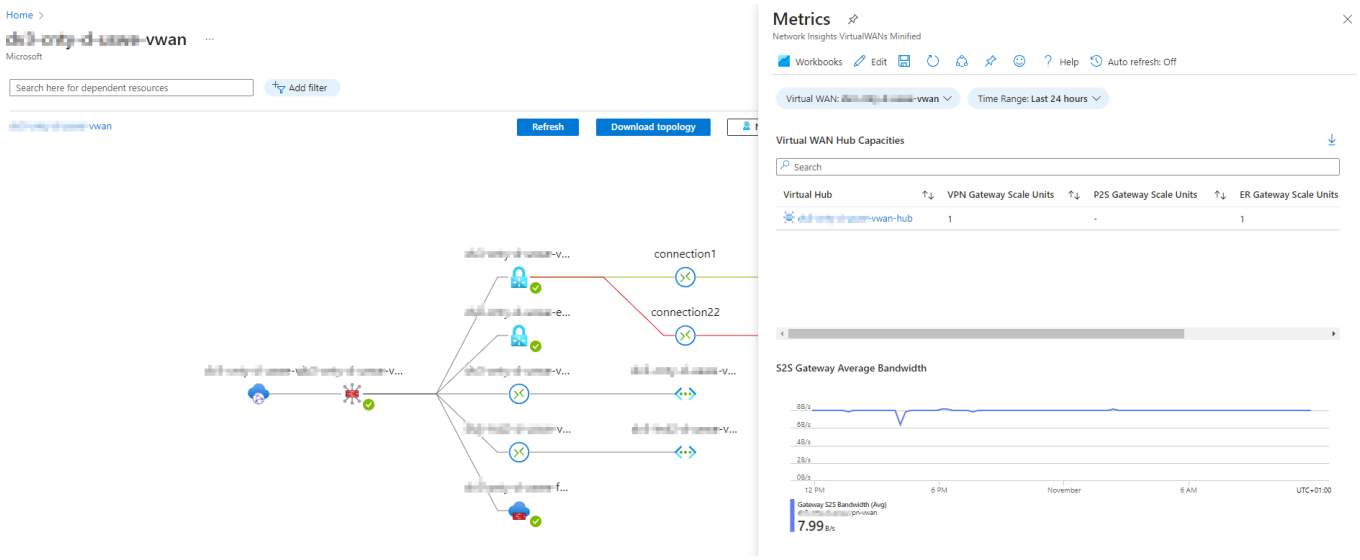
The **Virtual WAN Overviews [1]** part in the Overview blade as visible below shows an overview of the deployed Virtual WAN solutions.




The **Virtual WAN Resource Link [2]** column contains the Virtual WAN name as a link that will redirect to the Virtual WAN resource in Azure. The columns **Branch-To-Branch [3]** and **VNet-To-VNet [4]** show if branch to branch and vnet to vnet traffic is allowed for the virtual WAN.

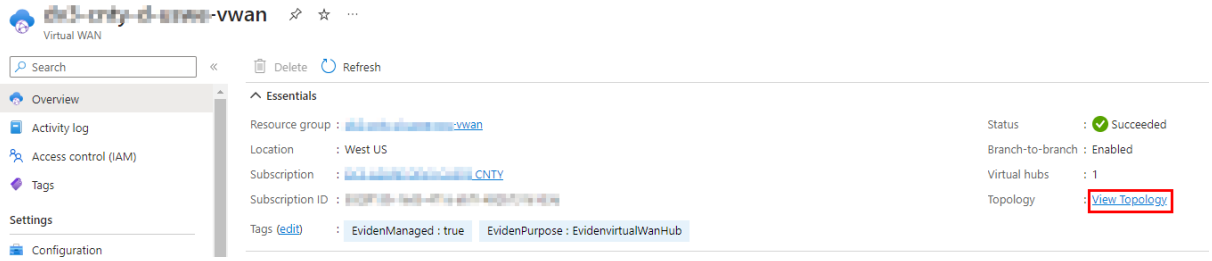
The **EvidenPurpose [5]** shows the value for the EvidenPurpose tag, while the **EvidenManaged [6]** column shows if the Virtual WAN is managed by Eviden or not.

In the last column, **Topology and metrics [7]**, a link is available to *View topology and metrics*. This link redirects to an overview that shows but the topology and the metrics blade for the selected Virtual WAN in the (default) Azure environment.



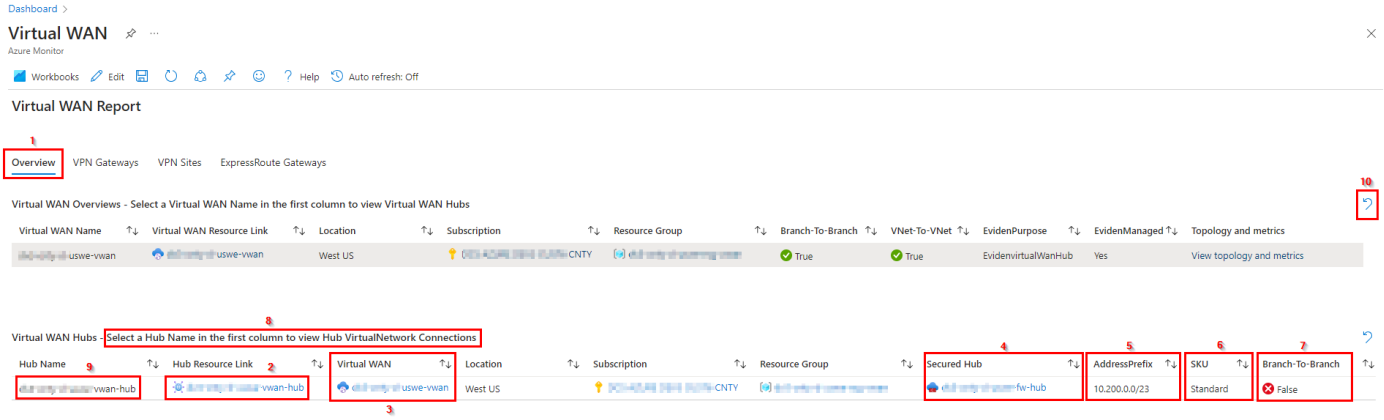

**Remark:** this blade can only be shown using this link if the Virtual WAN is same customer environment as is configured as the default (Startup) environment in Azure.

If the topology blade fails to load, first select the **Virtual WAN resource link [2]** in the overview and in the Virtual WAN resource link select **View Topology** as shown below to open this blade in Azure.




In the overview part of this blade there is the option to **Select a Virtual WAN Name in de first column to view Virtual WAN Hubs [8]**.

This means that you can select the name of the virtual WAN in the **Virtual WAN Name [9]** column and then the configured Virtual WAN Hubs for that virtual WAN are visible in the middle part of the **Overview [1]** blade, like in this picture:




Using the **counter wise pointing arrow [10]** the selection can be cleared, and the middle part of this blade will disappear again.

The **Hub Resource Link [2]** column contains the Virtual WAN Hub name as a link that will redirect to the Virtual WAN Hub resource in Azure. The column **Virtual WAN [3]** contains the name of the virtual WAN the hub is connected to and is provided as a link to the virtual WAN resource.

When the hub is secured by a firewall, the link to the firewall resource is provided in the **Secured Hub [4]** column.

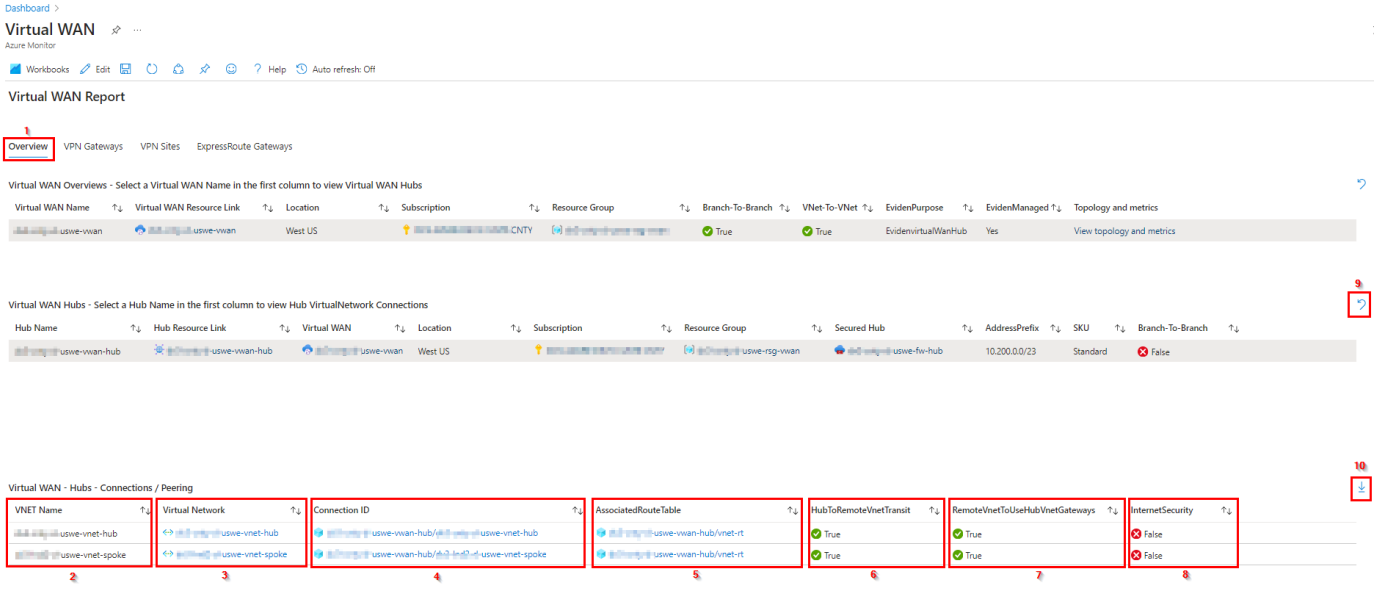
The **AddressPrefix [5]** column shows the private address space that is configured for the virtual hub.

In the **SKU [6]** column the hub type is shown. This can be **Basic** (for Site-to-site VPN configurations only) or **Standard** (support ExpressRoute, point-to-site (User VPN), a full mesh hub, and VNet-to-VNet transit through the Azure hubs).

**Branch-To-Branch [8]** show if branch to branch is allowed for the virtual hub.

In the middle part of this blade there is the option to **Select a Hub Name in the first column to view Hub VirtualNetwork Connections [8]**.

This means that you can select the name of the virtual hub in the **Hub Name [9]** column and then the configured hub virtual network connections for that virtual hub are visible in the bottom part of the **Overview [1]** blade, like in this picture:




With this bottom part the overview blade is complete. In the first column of this part the **VNet Name [2]** is shown followed by a **Virtual Network [3]** column that contains the link to the VNet. By clicking this link, you will be redirected to the virtual network blade in Azure.

The **Connection ID [4]** column shows the link to the hub virtual network connection, while the **AssociatedRouteTable [5]** column shows the link to the hub route table that is associated to the connection.

When the **HubToRemoteVNetTransit [6]** column shows **True**, virtual hub to remote vnet transit is enabled. **RemoteVnetToUseHubVnetGateways [7]** column shows if remote vnet to use virtual hub's gateways is allowed (**True**) or not (**False**).

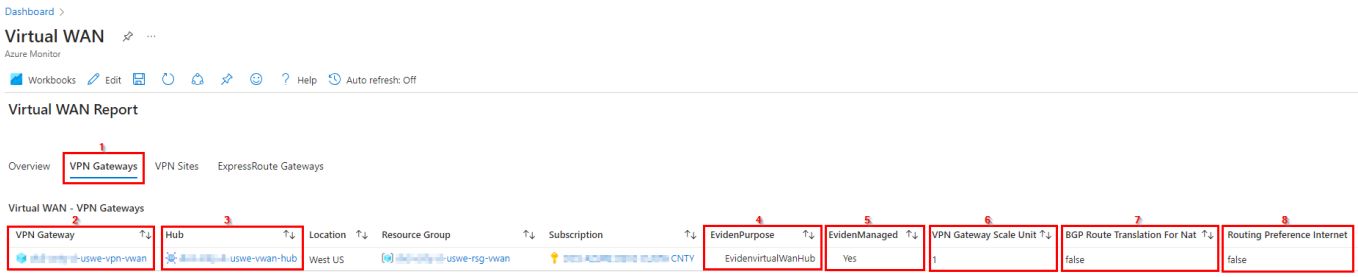
The **InternetSecurity [8]** column shows if internet security is enabled (**True**) for this connection or not (**False**).

Using the **counter wise pointing arrow [9]** the selection can be cleared, and the bottom part of this blade will disappear again.

When selecting the **down pointing arrow [10]**, the Virtual WAN – Hubs – Connections/Peering will be exported as a csv.

## 15.2 VPN Gateways blade

The **VPN Gateways [1]** blade as shown in the picture below, gives an overview of the VPN Gateways that are deployed in the environment.




The **VPN Gateway [2]** column shows the name of the VPN gateway provided as a link that redirects you to the resource blade for the VPN Gateway.

In the **Hub [3]** column the virtual hub, where the VPN Gateway is connected to is shown. This is also a link to the virtual hub resource blade in Azure.

The **EvidenPurpose [4]** shows the value for the EvidenPurpose tag, while the **EvidenManaged [5]** column shows if the Virtual WAN is managed by Eviden or not.

The **VPN Gateway Scale Unit [6]** column shows the number of scale units configured for the VPN Gateway. A scale unit is a unit defined to pick an aggregate throughput of a gateway in Virtual hub. 1 scale unit of VPN = 500 Mbps. 1 scale unit of ExpressRoute = 2 Gbps. Example: 10 scale unit of VPN would imply 500 Mbps * 10 = 5 Gbps.

**Enable BGP Route Translation For NAT [7]** shows if this setting is enabled (**True**) or not (**False**). For more information on this setting check this link.

The **Routing Preference Internet [8]** column shows if the routing preference is set to internet (**True**) or not (**False**). For more information on the routing preference setting check this link.

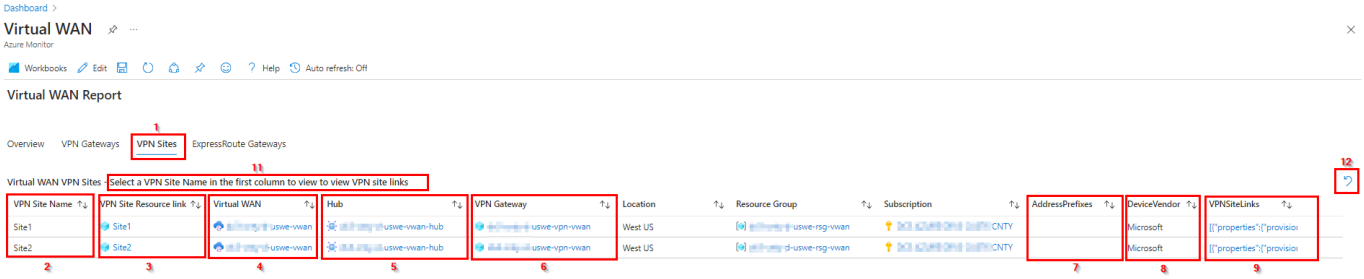
## 15.3 VPN Sites blade

The **VPN Sites [1]** blade provides an overview of the configured virtual wan vpn sites. For this this blade contains two parts:

- Virtual WAN VPN Sites
- Virtual WAN – VPN – Sites Links

When this blade is opened, only the top part appears as visible in the picture on the next page. This Virtual WAN VPN Sites overview will be described first.

In the **VPN Site Name [2]** column of this overview the name of the VPN Site is shown. In the **VPN Site Resource Link [3]** column the name of the VPN Site is shown as a link that will redirect to the VPN site blade in Azure.



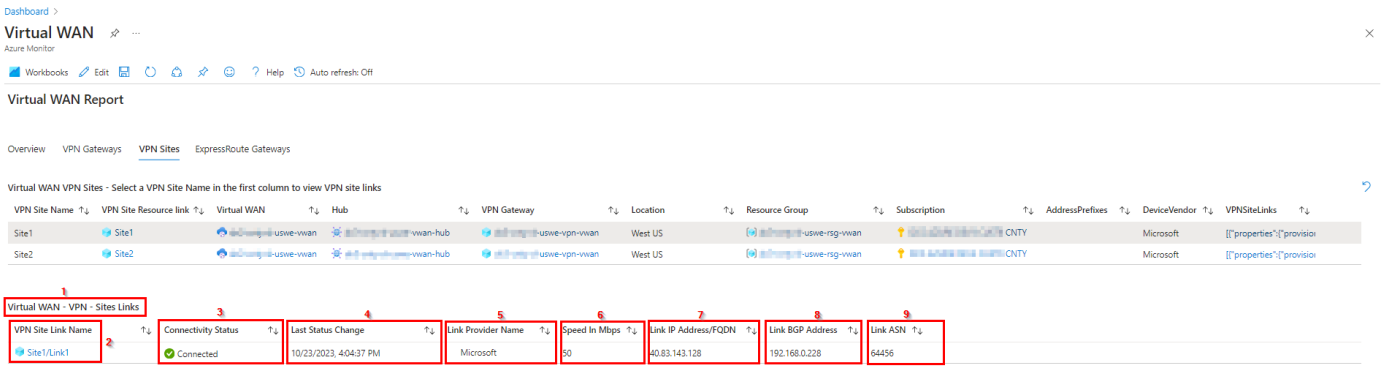

The columns **Virtual WAN [4]**, **Hub [5]** and **VPN Gateway [6]** show the links to the respective Virtual WAN, Hub and VPN Gateway the Site is connected to.

The **AddressPrefixes [7]** column show the configured address blocks, if any configured and the **DeviceVendor [8]** the name of the device vendor for the site-to-site connection. For more information on this and a list of device vendors check this link.

The **VPNSiteLinks [9]** column contains the properties of the site links in json format. When the properties are opened a detailed overview like this is opened:


When you **Select a VPN Site Name in the first column to view VPN site links [11]** a separate overview will show up at the bottom part of this blade with the VPN Site links. Using the **counter wise pointing arrow [12]** the selection can be cleared, and the bottom part of this blade will disappear again.

The VPN Sites blade with the **Virtual WAN - VPN - Sites Links [1]** part will look like this:



The first column shows the **VPN Site Link Name [2]**. This is a link that will redirect to the site/link blade in Azure.

The **Connectivity Status [3]** column shows the connectivity status of the link. As the connectivity status need to be checked separately it sometimes takes some time before the bottom part appears after the VPN Site Name is selected in the top part of this overview. In the **Last Status Change [4]** column, when this Connectivity Status was reached.

The **Link Provider Name [5]** shows the name of the vendor that provides the link and is in most cases the same as the DeviceVendor as shown in the top part of this blade.

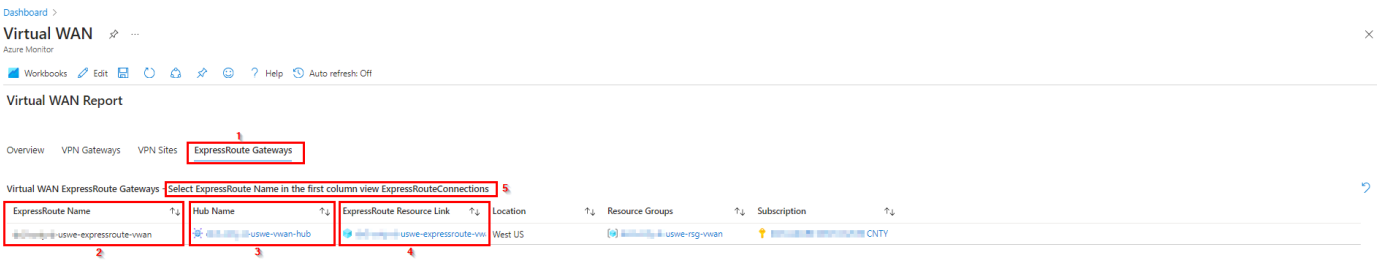
The next colums show the configuration information for the link like **Speed in Mbps [6]**, **Link IP Address/FQDN [7]**, **Link BGP Address [8]** and **Link ASN [9].**

## 15.4 ExpressRoute Gateways blade

The **ExpressRoute Gateways [1]** blade provides an overview of the configured ExpressRoute Gateways. For this this blade contains two parts:

- Virtual WAN ExpressRoute Gateways
- Virtual WAN - ExpressRoute Connection List

When this blade is opened, only the top part appears as visible in the picture on the next page. This Virtual WAN ExpressRoute Gateways overview will be described first.

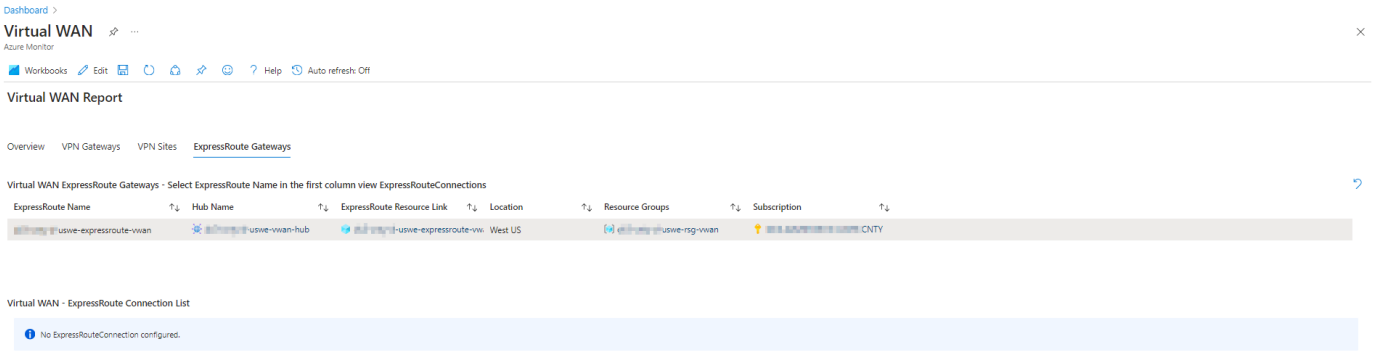



The **ExpressRoute Name [2]** shows the name of the ExpressRoute gateway, while in the **ExpressRoute Resource Link [4]** column the link to the ExpressRoute Azure blade can be found.

In the **Hub Name [3]** column the link to the Virtual Hub where the ExpressRoute Gateway is connected to is shown.

In this overview you can **Select ExpressRoute Name in the first column view ExpressRouteConnections [5]** to get an overview of the ExpressRoute

connections for the selected ExpresRoute gateway in the bottompart of this overview.




In this example there are no ExpressRoute Connections available due to the costs of these connections, but in case they are configured the following columns will be visible in for the connections:

- **ExpressRoute Connection**: a link to the ExpressRoute Connection blade in Azure.
- **ExpressRouteCircuitPeering**: This can be Private or Microsoft peering. Check this link for more information on this.
- **RoutingWeight**: shows the connection weight of this ExpressRoute connection. For more information check this link.
- **Enable Internet Security**: Enable internet security. The value can be **True** or **False**.
- **ExpressRouteGatewayBypass**: Enable FastPath to vWan Firewall hub. The value can be **True** or **False**.
- **RoutingConfiguration**: The Routing Configuration indicating the associated and propagated route tables on this connection.