XTS Views and Queries

Last updated by | Vitor Tomaz | Aug 5, 2020 at 12:44 PM PDT

Contents

Background

XTS provides you access to cluster information and is used in troubleshooting issues in the environment. This document will take you through the process of installing it, configuring it for your environment, and show how to use the VA XTS view.

XTS Installation

1. Open a new PowerShell window in Administrative mode

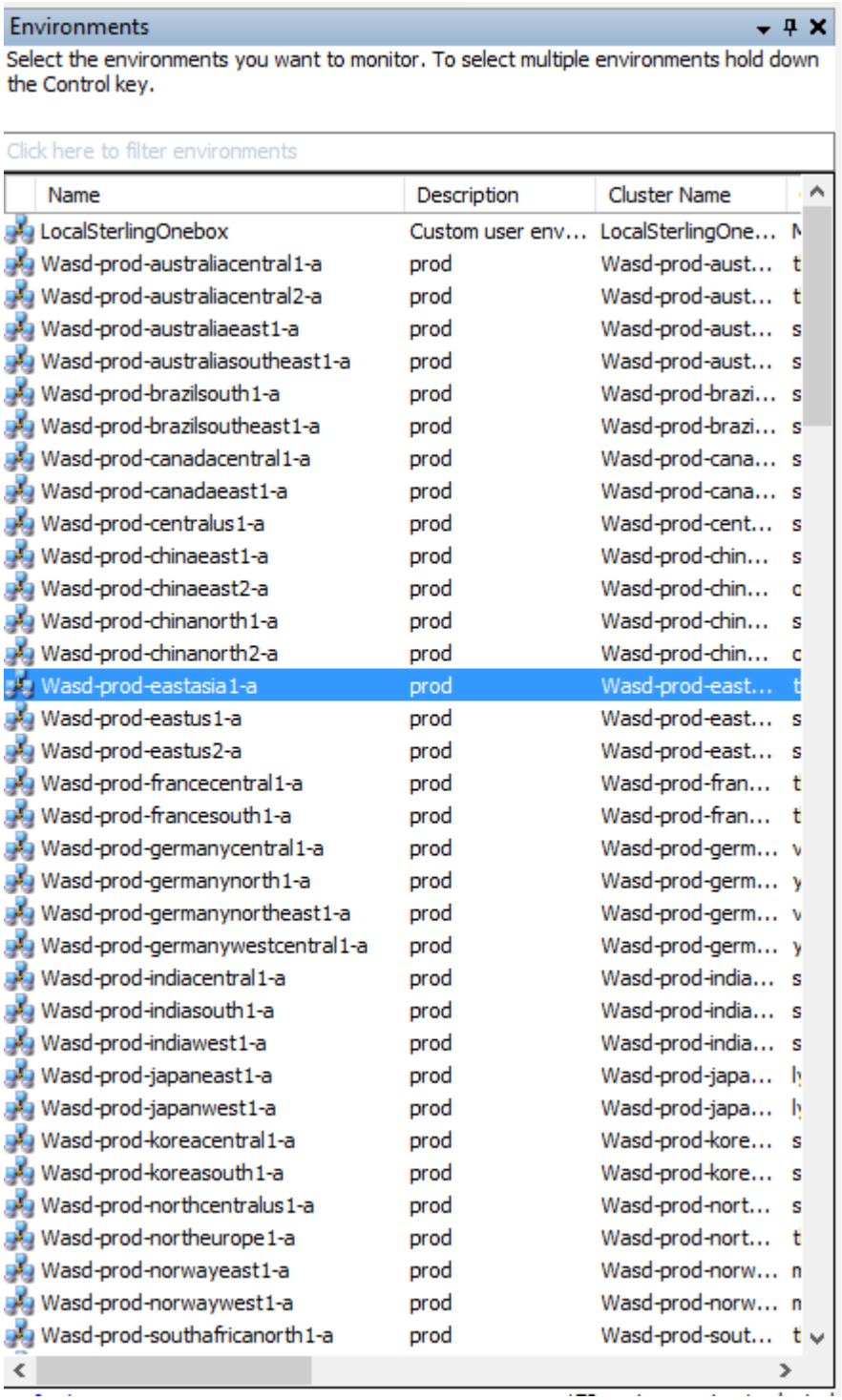
```
# Install the Azure Resource Manager modules from the PowerShell Gallery
Install-Module AzureRM -Scope CurrentUser
# Install the Azure Service Management module from the PowerShell Gal
# (may need to add the -AllowClobber parameter to overwrite redundant cmdlets from AzureRM) e83baee77f65
```

2. Install XTS from: link: \sqlcl\Team\ServicePlatform\release\XTS

XTS Basic Usage

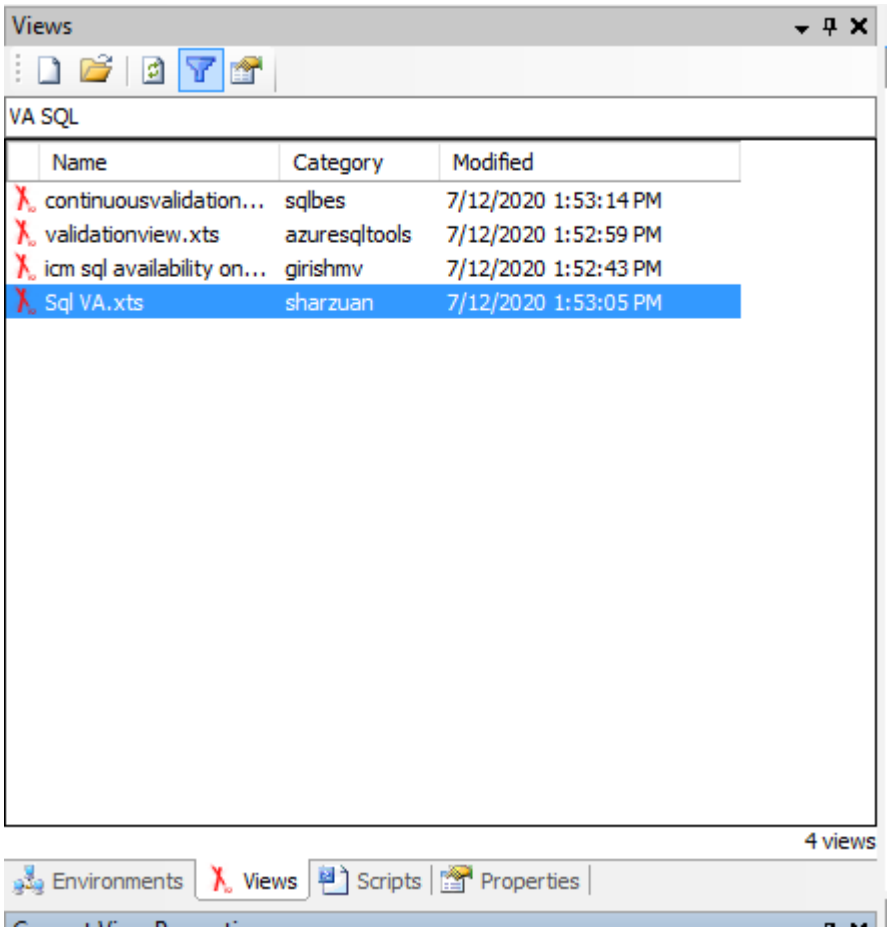
Environment Selection

This is where you select which environment you want to view. Note The filter bar here to filter the list and find what you need faster. It is used in many areas throughout XTS.



View Selection

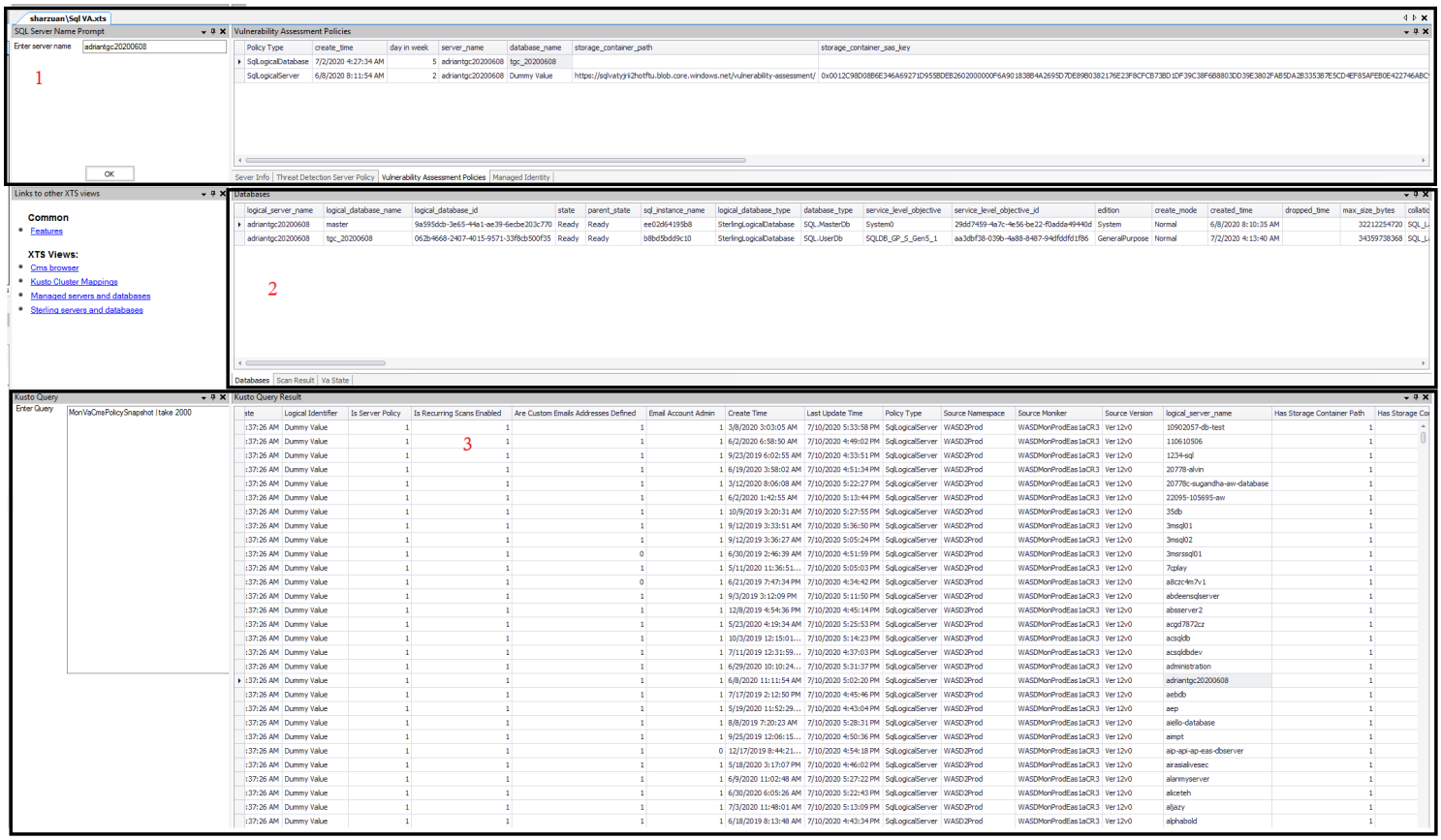
This is where you select which view you want to view. Note The filter bar here to filter the list and find what you need faster - in our case, we will select "Sql Va" view.



SQL Va View

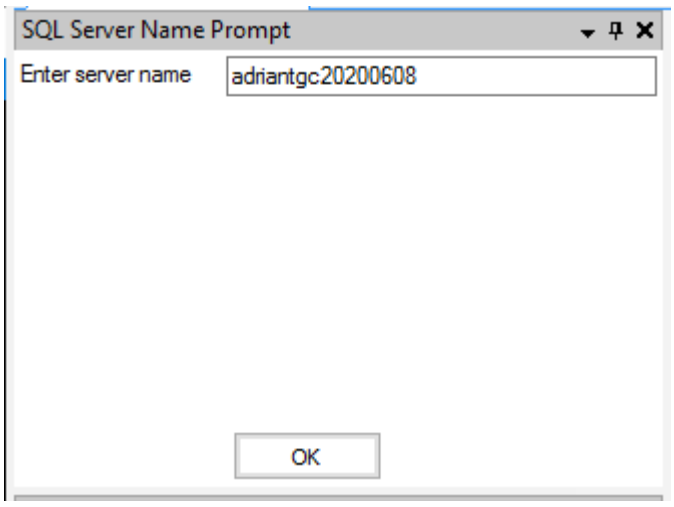
The view divided into 3 main part -

1. Server level and policy info
2. Database level info
3. Kusto data



Server level and policy info

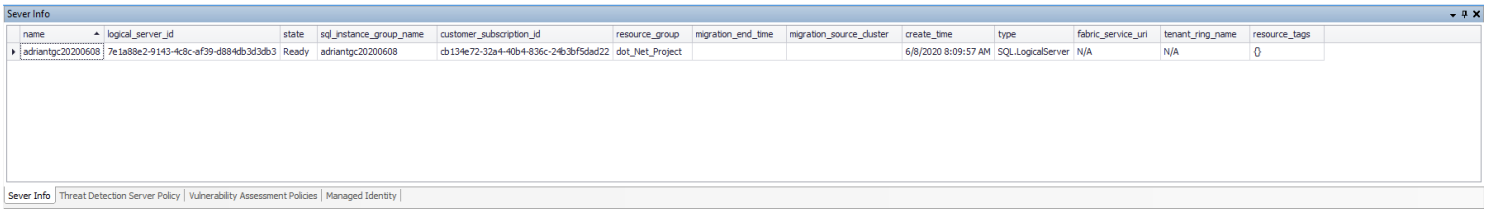
In this view we can see a data related to the server and server policies First, insert to 'SQL server name prompt' the server name and press OK.



This action will set the view to display data for the selected server (you can write a SQL server or a managed instance server).

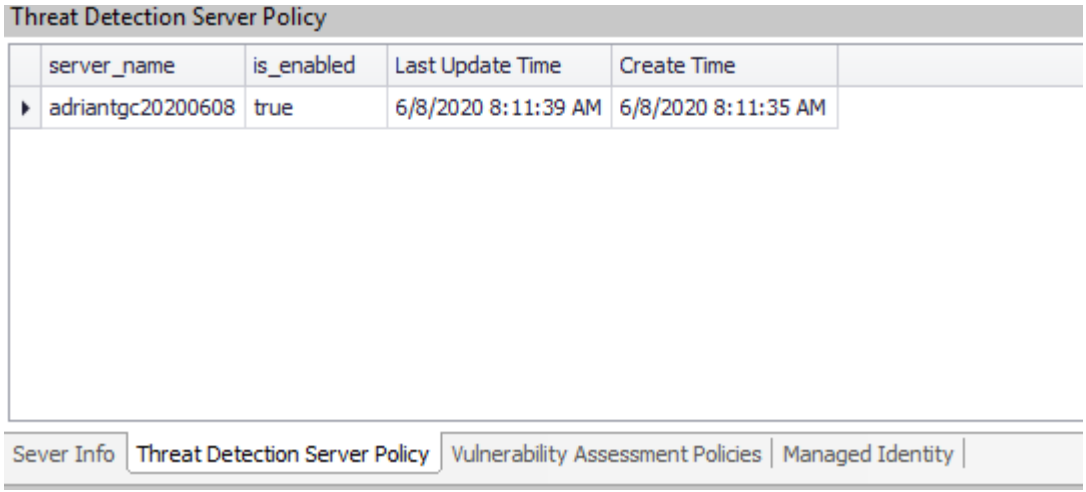
Server info tab

This tab display server general information such as - server id, subscription, resource group and more.



Threat Detection Server Policy tab

In this tab we can know if the ADS was enable and when. The pre condtinon for Vulnerability assessment service is that ADS be enabled.

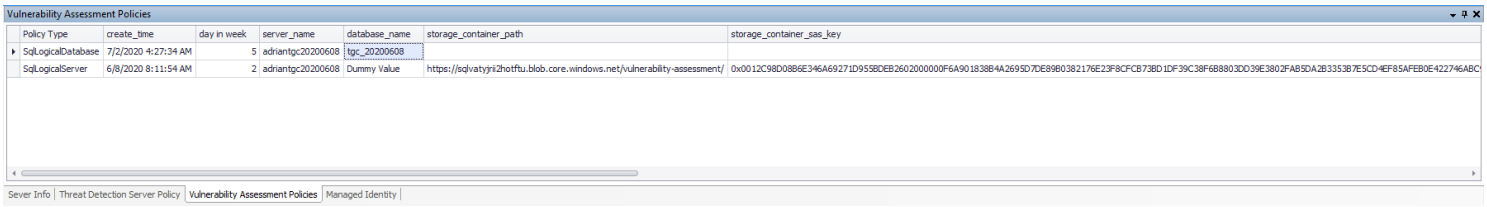


Vulnerability Assessment Policies tab

In this tab, we can know if the server/databases have a Vulnerability assessment policy. Vulnerability assessment must have a definition of 'storage container path', in this container the Vulnerability assessment (VA) output will be saved. The VA service must have permission to assess the storage container. There is two way for VA service accesses to the storage -

1. Using storage container SAS key - We can see if there is a SAS key in the 'storage _container_sas_key' column.
2. Using Managed Identity - if the 'storage _container_sas_key' column is empty (for all the rows) the VA service used Managed Identity (to check Managed Identity definition we need to go to 'Managed Identity' tab).

Note - The VA service first check if SAS key is define and if isn't try to used the server Managed Identity.



Managed Identity tab

I this tab we can see if the server has a Managed Identity and if it is set properly For Managed Identity set properly the following conditions must be met:

1. subscription_tenant_id and server_identity_tenant_id must be equal - if them not equal the subscription was moved from one tenant to another tenant, all identities under previous tenant were not moved to new tenant (link for mitigation)
2. server_identity_principal_id and server_identity_url they must not be empty.
3. certificate_was_created must be true.

server_name	server_subscription_id	subscription_tenant_id	server_identity_tenant_id	server_identity_principal_id	server_identity_url
csbphdrsqlmib	28efc852-00e9-41ac-b216-6f02351239c3	d5d2540f-f60a-45ad-86a9-e2e792ee6669	d5d2540f-f60a-45ad-86a9-e2e792ee6669	e344526c-adbf-452e-98cc-20a2ead1d466	https://control-eastasia.identity.azure.net/subscriptions/28efc852-00e9-41ac-b216-6f02351239c3/resourcegroups/CsbPhDrSqlMRG-B/providers/Microsoft.Sql/managedIr

Sever Info | Threat Detection Server Policy | Vulnerability Assessment Policies | Managed Identity

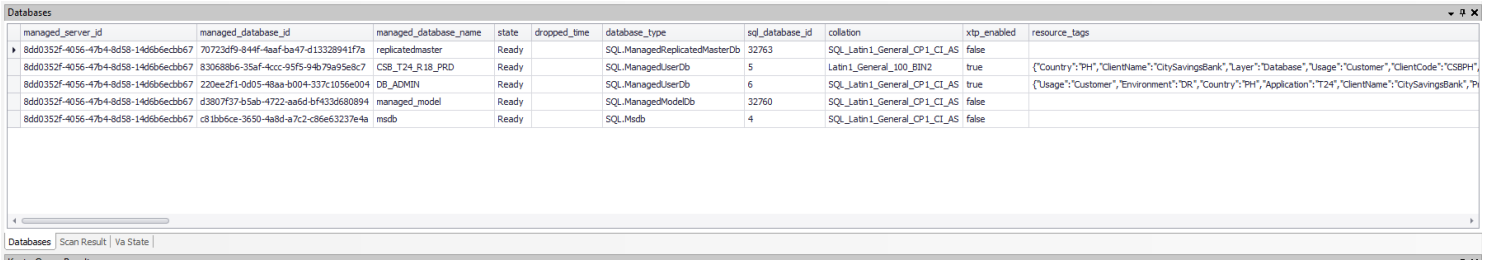
For Managed Identity error mitigation go to link

Database level info

This section display information of the databases and extended data for the Vulnerability Assessment service to each database.

Databases tab

This view display for each database in the selected server a general information.



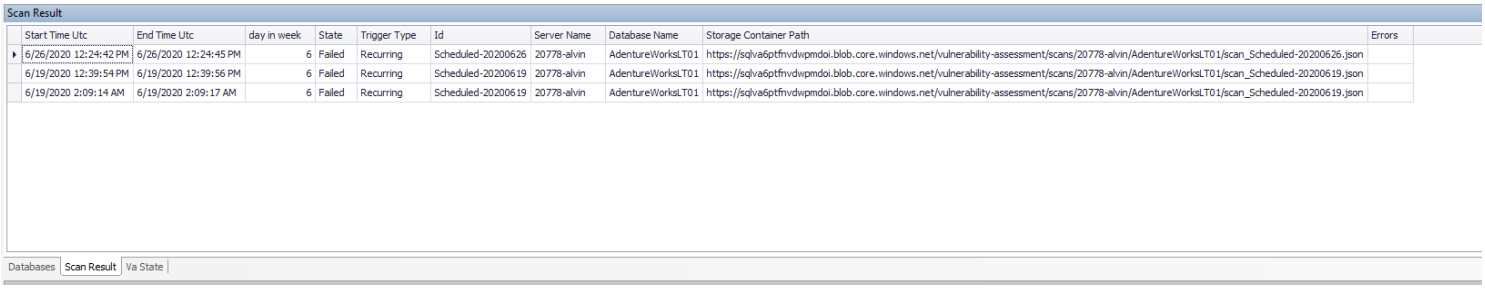
Databases

managed_server_id	managed_database_id	managed_database_name	state	dropped_time	database_type	sql_database_id	collation	xtp_enabled	resource_tags
8dd0352f-4056-47b4-8d58-14d6b6ecbb67	70723df9-844f-4aaf-ba47-d13328941f7a	replicatedmaster	Ready		SQL.ManagedReplicatedMasterDb	32763	SQL_Latin1_General_CP1_CI_AS	false	
8dd0352f-4056-47b4-8d58-14d6b6ecbb67	830688b6-35af-4ccc-95f5-94b79a95e8c7	CSB_T24_R18_PRD	Ready		SQL.ManagedUserDb	5	Latin1_General_100_BIN2	true	{"Country":"PH","ClientName":"CitySavingsBank","Layer":"Database","Usage":"Customer","ClientCode":"CSBPH",
8dd0352f-4056-47b4-8d58-14d6b6ecbb67	220ee2f1-0d05-48aa-b004-337c1056e004	DB_ADMIN	Ready		SQL.ManagedUserDb	6	SQL_Latin1_General_CP1_CI_AS	true	{"Usage":"Customer","Environment":"DR","Country":"PH","Application":"T24","ClientName":"CitySavingsBank","Pl
8dd0352f-4056-47b4-8d58-14d6b6ecbb67	d3807f37-b5ab-4722-aa6d-bf433d680894	managed_model	Ready		SQL.ManagedModelDb	32760	SQL_Latin1_General_CP1_CI_AS	false	
8dd0352f-4056-47b4-8d58-14d6b6ecbb67	c81bb6ce-3650-4a8d-a7c2-c86e63237e4a	msdb	Ready		SQL.Msdb	4	SQL_Latin1_General_CP1_CI_AS	false	

Databases | Scan Result | Va State

Scan result tab

First, We must select a database from the 'Databases tab' (you can also select a database from the 'Vulnerability Assessment Policies tab'). This view displays a list of VA scans performed on the selected database.



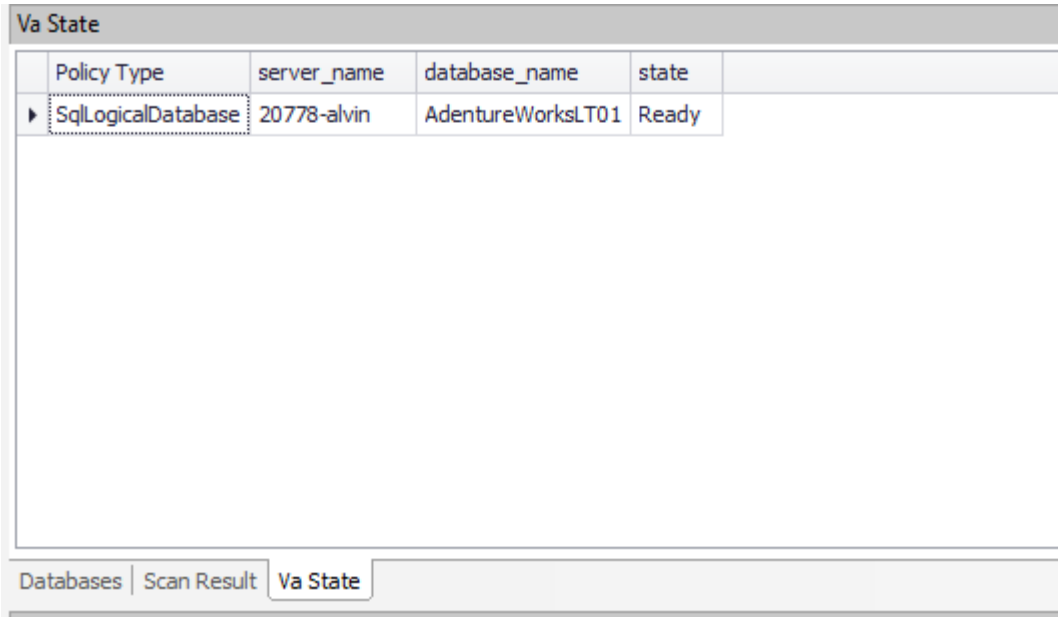
Scan Result

Start Time Utc	End Time Utc	day in week	State	Trigger Type	Id	Server Name	Database Name	Storage Container Path	Errors
6/26/2020 12:24:42 PM	6/26/2020 12:24:45 PM	6	Failed	Recurring	Scheduled-20200626	20778-alvin	AdentureWorksLT01	https://sqlva6ptfnvdwpmdoi.blob.core.windows.net/vulnerability-assessment/scans/20778-alvin/AdentureWorksLT01/scan_Scheduled-20200626.json	
6/19/2020 12:39:54 PM	6/19/2020 12:39:56 PM	6	Failed	Recurring	Scheduled-20200619	20778-alvin	AdentureWorksLT01	https://sqlva6ptfnvdwpmdoi.blob.core.windows.net/vulnerability-assessment/scans/20778-alvin/AdentureWorksLT01/scan_Scheduled-20200619.json	
6/19/2020 2:09:14 AM	6/19/2020 2:09:17 AM	6	Failed	Recurring	Scheduled-20200619	20778-alvin	AdentureWorksLT01	https://sqlva6ptfnvdwpmdoi.blob.core.windows.net/vulnerability-assessment/scans/20778-alvin/AdentureWorksLT01/scan_Scheduled-20200619.json	

Databases | Scan Result | Va State

Va State tab

This view displays the Vulnerability Assessment state for each database.

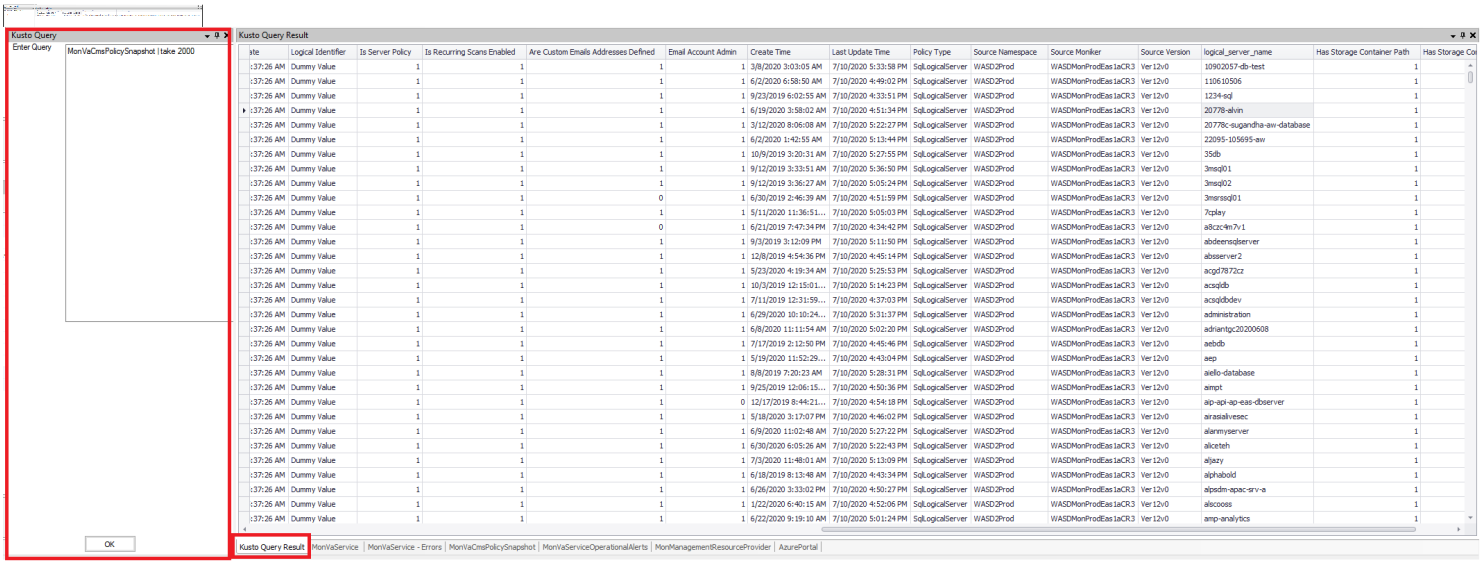


Kusto data

The section displays a set of Kusto queries results.

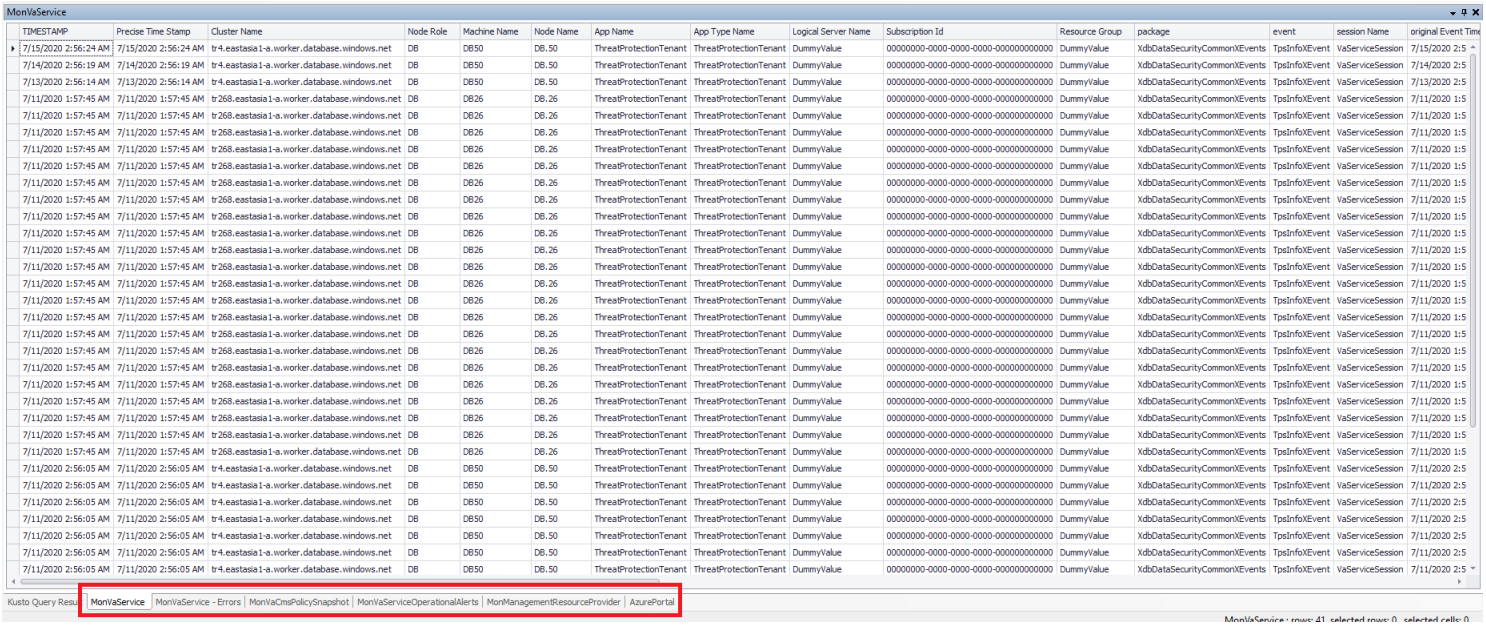
Free Search bar

We can use the Kusto query text box to run any query we want, the result will display on the 'Kusto Query Result' tab.



Static Kusto query

The other tabs displays a predefined queries result



How good have you found this content?