

XTS Views and Queries

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

Contents

- [Background](#)
 - [XTS Installation](#)
- [XTS Basic Usage](#)
 - [Environment Selection](#)
 - [View Selection](#)
- [SQL Va View](#)
 - [Server level and policy info](#)
 - [Server info tab](#)
 - [Threat Detection Server Policy tab](#)
 - [Vulnerability Assessment Policies tab](#)
 - [Managed Identity tab](#)
 - [Database level info](#)
 - [Databases tab](#)
 - [Scan result tab](#)
 - [Va State tab](#)
 - [Kusto data](#)
 - [Free Search bar](#)
 - [Static Kusto query](#)

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.

Environments

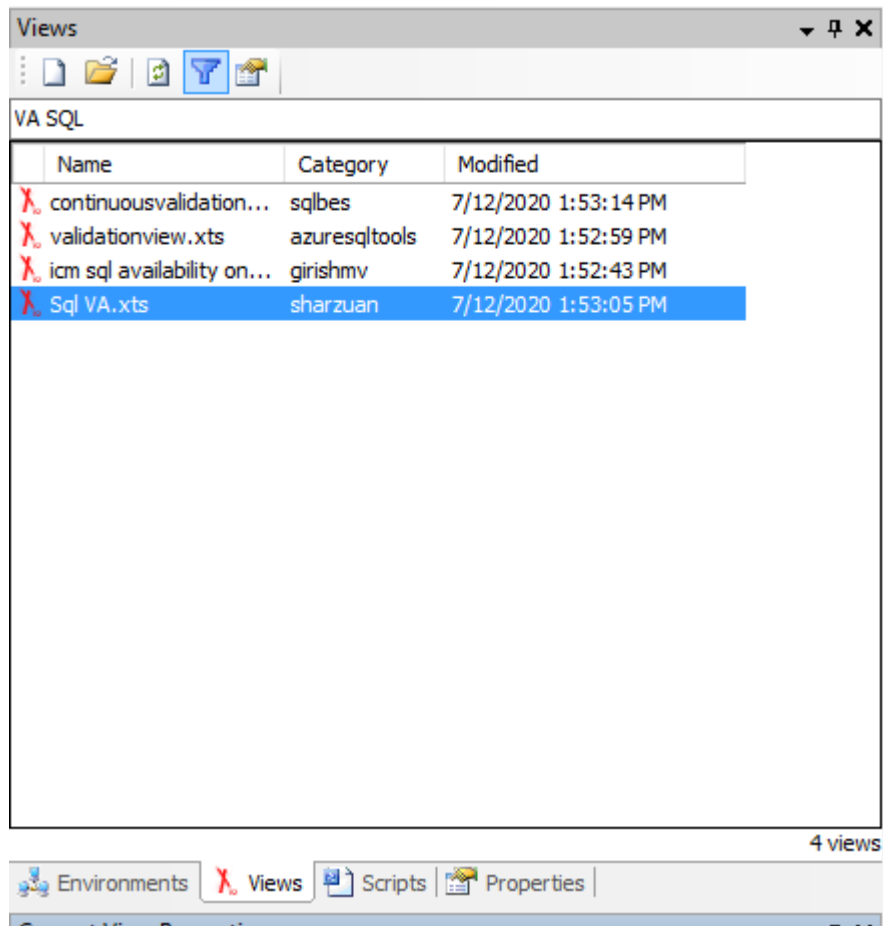
Select the environments you want to monitor. To select multiple environments hold down the Control key.

Click here to filter environments

Name	Description	Cluster Name
LocalSterlingOnebox	Custom user env...	LocalSterlingOne...
Wasd-prod-australiacentral1-a	prod	Wasd-prod-aust...
Wasd-prod-australiacentral2-a	prod	Wasd-prod-aust...
Wasd-prod-australiaeast1-a	prod	Wasd-prod-aust...
Wasd-prod-australiasoutheast1-a	prod	Wasd-prod-aust...
Wasd-prod-brazilsouth1-a	prod	Wasd-prod-brazi...
Wasd-prod-brazilsoutheast1-a	prod	Wasd-prod-brazi...
Wasd-prod-canadacentral1-a	prod	Wasd-prod-cana...
Wasd-prod-canadaeast1-a	prod	Wasd-prod-cana...
Wasd-prod-centralus1-a	prod	Wasd-prod-cent...
Wasd-prod-chinaeast1-a	prod	Wasd-prod-chin...
Wasd-prod-chinaeast2-a	prod	Wasd-prod-chin...
Wasd-prod-chinanorth1-a	prod	Wasd-prod-chin...
Wasd-prod-chinanorth2-a	prod	Wasd-prod-chin...
Wasd-prod-eastasia1-a	prod	Wasd-prod-east...
Wasd-prod-eastus1-a	prod	Wasd-prod-east...
Wasd-prod-eastus2-a	prod	Wasd-prod-east...
Wasd-prod-francecentral1-a	prod	Wasd-prod-fran...
Wasd-prod-francesouth1-a	prod	Wasd-prod-fran...
Wasd-prod-germanycentral1-a	prod	Wasd-prod-germ...
Wasd-prod-germanynorth1-a	prod	Wasd-prod-germ...
Wasd-prod-germanynortheast1-a	prod	Wasd-prod-germ...
Wasd-prod-germanywestcentral1-a	prod	Wasd-prod-germ...
Wasd-prod-indiacentral1-a	prod	Wasd-prod-india...
Wasd-prod-indiasouth1-a	prod	Wasd-prod-india...
Wasd-prod-indiawest1-a	prod	Wasd-prod-india...
Wasd-prod-japaneast1-a	prod	Wasd-prod-japa...
Wasd-prod-japanwest1-a	prod	Wasd-prod-japa...
Wasd-prod-koreacentral1-a	prod	Wasd-prod-kore...
Wasd-prod-koreasouth1-a	prod	Wasd-prod-kore...
Wasd-prod-northcentralus1-a	prod	Wasd-prod-nort...
Wasd-prod-northeurope1-a	prod	Wasd-prod-nort...
Wasd-prod-norwayeast1-a	prod	Wasd-prod-norw...
Wasd-prod-norwaywest1-a	prod	Wasd-prod-norw...
Wasd-prod-southafricanorth1-a	prod	Wasd-prod-sout...

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

1. SQL Server Name Prompt

Enter server name:

OK

2. Vulnerability Assessment Policies

Policy Type	create_time	day in week	server_name	database_name	storage_container_path	storage_container_key
SqlLogicalDatabase	7/2/2020 4:27:34 AM	5	adriantgc20200608	tpc_20200608		
SqlLogicalServer	6/8/2020 8:11:54 AM	2	adriantgc20200608	Dummy Value	https://sqlvstgyn2hoftu.blob.core.windows.net/vulnerability-assessment/	0x0012C38D08B6E346A69271D955DEB260200000F6A90183884A2695D7DE980382176E23F8CF873801DF39C39F688803D03802FAB5DA2B33387E5CD4EF85AF80E422746AB0C

3. Kusto Query Result

Logical Identifier	Is Server Policy	Is Recurring Scans Enabled	Are Custom Emails Addresses Defined	Email Account Admin	Create Time	Last Update Time	Policy Type	Source Namespace	Source Monitor	Source Version	logical_server_name	Has Storage Container Path	Has Storage Co
137-26 AM Dummy Value	1	1	1	1	1/28/2020 3:02:05 AM	7/10/2020 5:33:58 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	10902057-db-test	1	
137-26 AM Dummy Value	1	1	1	1	1/6/2020 6:58:50 AM	7/10/2020 4:49:02 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	115610556	1	
137-26 AM Dummy Value	1	1	1	1	1/9/2019 6:02:55 AM	7/10/2020 4:33:51 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	1234-adj	1	
137-26 AM Dummy Value	1	1	1	1	1/6/19/2020 3:58:02 AM	7/10/2020 4:51:34 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	20778-shin	1	
137-26 AM Dummy Value	1	1	1	1	1/3/12/2020 8:06:08 AM	7/10/2020 5:22:27 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	20778-sugandha-ai-database	1	
137-26 AM Dummy Value	1	1	1	1	1/6/2020 1:42:53 AM	7/10/2020 5:13:44 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	22095-105695-aw	1	
137-26 AM Dummy Value	1	1	1	1	1/10/2019 3:20:31 AM	7/10/2020 5:27:55 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	35db	1	
137-26 AM Dummy Value	1	1	1	1	1/9/12/2019 3:33:51 AM	7/10/2020 5:36:30 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	3meq01	1	
137-26 AM Dummy Value	1	1	1	1	1/9/12/2019 3:36:27 AM	7/10/2020 5:05:24 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	3meq02	1	
137-26 AM Dummy Value	1	1	1	0	1/6/2019 2:46:39 AM	7/10/2020 4:51:59 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	3mreq01	1	
137-26 AM Dummy Value	1	1	1	1	1/5/11/2020 11:36:51...	7/10/2020 5:05:03 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	7play	1	
137-26 AM Dummy Value	1	1	1	0	1/6/12/2019 7:47:34 PM	7/10/2020 4:54:42 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	adccen7v1	1	
137-26 AM Dummy Value	1	1	1	1	1/9/2019 3:12:09 PM	7/10/2020 5:11:50 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	abderudserver	1	
137-26 AM Dummy Value	1	1	1	1	1/12/8/2019 4:54:36 PM	7/10/2020 4:45:14 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	abserver2	1	
137-26 AM Dummy Value	1	1	1	1	1/5/23/2020 4:19:34 AM	7/10/2020 5:25:53 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	acqf787cz	1	
137-26 AM Dummy Value	1	1	1	1	1/10/2019 12:15:01...	7/10/2020 5:14:23 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	acqfdb	1	
137-26 AM Dummy Value	1	1	1	1	1/7/11/2019 12:31:59...	7/10/2020 4:37:03 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	acqfdbdev	1	
137-26 AM Dummy Value	1	1	1	1	1/6/29/2020 10:10:24...	7/10/2020 5:31:37 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	administration	1	
137-26 AM Dummy Value	1	1	1	1	1/6/8/2020 11:11:54 AM	7/10/2020 5:02:20 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	adriantgc20200608	1	
137-26 AM Dummy Value	1	1	1	1	1/7/17/2019 2:12:50 PM	7/10/2020 4:45:46 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	aedb	1	
137-26 AM Dummy Value	1	1	1	1	1/5/19/2020 11:52:26...	7/10/2020 4:43:04 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	aep	1	
137-26 AM Dummy Value	1	1	1	1	1/8/8/2019 7:20:23 AM	7/10/2020 5:28:31 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	aello-database	1	
137-26 AM Dummy Value	1	1	1	1	1/9/25/2019 12:06:15...	7/10/2020 4:50:36 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	ampt	1	
137-26 AM Dummy Value	1	1	1	1	0/12/17/2019 8:46:21...	7/10/2020 4:54:18 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	ap-ap-ap-ap-ear-observer	1	
137-26 AM Dummy Value	1	1	1	1	1/5/18/2020 5:17:07 PM	7/10/2020 4:46:02 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	aresalivsec	1	
137-26 AM Dummy Value	1	1	1	1	1/6/20/2020 11:02:48 AM	7/10/2020 5:27:22 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	armysserver	1	
137-26 AM Dummy Value	1	1	1	1	1/6/30/2020 6:05:26 AM	7/10/2020 5:22:43 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	alceah	1	
137-26 AM Dummy Value	1	1	1	1	1/7/3/2020 11:48:01 AM	7/10/2020 5:13:09 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	aljay	1	
137-26 AM Dummy Value	1	1	1	1	1/6/18/2019 8:13:48 AM	7/10/2020 4:43:34 PM	SqlLogicalServer	WASD2Prod	WASDMonProdEasIaCR3	Ver12v0	alphabold	1	

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.

SQL Server Name Prompt

Enter server name:

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.

Server Info												
name	logical_server_id	state	sql_instance_group_name	customer_subscription_id	resource_group	migration_end_time	migration_source_cluster	create_time	type	fabric_service_uri	tenant_ring_name	resource_tags
adriantgc20200608	7e1a89e2-9143-4c8c-ef39-d884db3d3db3	Ready	adriantgc20200608	cb134e72-32a4-40b4-836c-24b3bf5dad22	dot_Net_Project			6/8/2020 8:09:57 AM	SQL_LogicalServer	N/A	N/A	0

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

Threat Detection Server Policy tab

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

Threat Detection Server Policy				
server_name	is_enabled	Last Update Time	Create Time	
adriantgc20200608	true	6/8/2020 8:11:39 AM	6/8/2020 8:11:35 AM	

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

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.

Vulnerability Assessment Policies						
Policy Type	create_time	day in week	server_name	database_name	storage_container_path	storage_container_sas_key
SqlLogicalDatabase	7/2/2020 4:27:34 AM	5	adriantgc20200608	tpc_20200608		
SqlLogicalServer	6/8/2020 8:11:54 AM	2	adriantgc20200608	Dummy Value	https://sqlvatyri2hotffu.blob.core.windows.net/vulnerability-assessment/	0x0012C98D0886E346A69271D9558DEB260200000F6A90183884A2695D70E99B0382176E23F8CFCB73BD1DF39C38F6B88030C39E3802FAB5DA2B3353B7E5CD4EF85AFEB0E422746ABC

Server Info | Threat Detection Server Policy | Vulnerability Assessment Policies | 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
cbphdrgslmb	28efc852-00e9-41ac-b216-6f02351239c3	d5d2540f-f60a-45ad-86a9-e2e792ee6669	d5d2540f-f60a-45ad-86a9-e2e792ee6669	e344525c-adbf-452e-98cc-20a2ead1d466	https://control-eastasia.identity.azure.net/subscriptions/28efc852-00e9-41ac-b216-6f02351239c3/resourcegroups/CbPhDrSgMRG-R/providers/Microsoft.Sql/managedIdentity

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.

managed_server_id	managed_database_id	managed_database_name	state	dropped_time	database_type	sql_database_id	collation	xtp_enabled	resource_tags
8d0332f-4056-47b4-8d58-14d6b6ecb667	70723d9f-844f-4aaf-ba47-d13328941f7a	replicatedmaster	Ready		SQL_ManagedReplicatedMasterDb	32763	SQL_Latin1_General_CP1_CI_AS	false	
8d0332f-4056-47b4-8d58-14d6b6ecb667	830688b6-35ef-4ccc-95f5-94b79a95ebc7	C3B_T24_R_1B_PRD	Ready		SQL_ManagedUserDb	5	Latin1_General_100_BIN2	true	["Country": "PH", "ClientName": "CitySavingsBank", "Layer": "Database", "Usage": "Customer", "ClientCode": "C3BPH"]
8d0332f-4056-47b4-8d58-14d6b6ecb667	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", "P"]
8d0332f-4056-47b4-8d58-14d6b6ecb667	d3807f37-b5ab-4722-aa6d-bf433d680894	managed_model	Ready		SQL_ManagedModelDb	32760	SQL_Latin1_General_CP1_CI_AS	false	
8d0332f-4056-47b4-8d58-14d6b6ecb667	c81bb6ce-3650-4a8d-a7c2-c86e63237e4a	msdb	Ready		SQL_Msdb	4	SQL_Latin1_General_CP1_CI_AS	false	

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.

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	AdventureWorksLT01	https://sqlva6ptfndvdpmdoi.blob.core.windows.net/vulnerability-assessment/scans/20778-alvin/AdventureWorksLT01/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	AdventureWorksLT01	https://sqlva6ptfndvdpmdoi.blob.core.windows.net/vulnerability-assessment/scans/20778-alvin/AdventureWorksLT01/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	AdventureWorksLT01	https://sqlva6ptfndvdpmdoi.blob.core.windows.net/vulnerability-assessment/scans/20778-alvin/AdventureWorksLT01/scan_Scheduled-20200619.json	

Va State tab

This view displays the Vulnerability Assessment state for each database.

7/8

MonVaService: rows: 41 selected rows: 0 selected cells: 0