itm8 Databasens dag

Microsoft SQL Server Security

Steen Cornelius

Today. Tomorrow. Together

AGENDA

01. SQL Server version

02. Azure Arc

03. Configure

04. Clients

05. EXECUTE AS

06. Proxies

07. Vulnerability Assessment

08. xEvents

09.

10.

SQL Server version (Onprem)

- SQL Server 2022, SQL Server 2019 or SQL Server 2017
- SQL Server 2016, SQL Server 2014, SQL Server 2012 or SQL Server 2008 R2

https://sqlserverbuilds.blogspot.com

Azure Arc

Azure Arc Enable

Helps Onprem SQL Server
SQL Server 2012 and newer with SU

itm8

Configure

SQL Server Management Studio (SSMS)

Facets

- Server Security
- Surface Area Configuration

Group-Managed Service Accounts - gMSA

Clients

Always Encrypted with Secure Enclaves

- Has a performance cost

Clients

Strict Encryption

requires

ODBC 18 Driver for SQL Server

Microsoft OLE DB Driver 19 for SQL Server

EXECUTE AS

Stored Procedures in another user’s security context

EXECUTE AS

```sql
CREATE PROCEDURE HumanResources.uspEmployeesInDepartment @DeptValue INT
    WITH EXECUTE AS OWNER
AS
SET NOCOUNT ON;

SELECT e.BusinessEntityID,
    c.LastName,
    c.FirstName,
    e.JobTitle
FROM Person.Person AS c
INNER JOIN HumanResources.Employee AS e
    ON c.BusinessEntityID = e.BusinessEntityID
INNER JOIN HumanResources.EmployeeDepartmentHistory AS edh
    ON e.BusinessEntityID = edh.BusinessEntityID
WHERE edh.DepartmentID = @DeptValue
ORDER BY c.LastName,
    c.FirstName;
GO

-- Execute the stored procedure by specifying department 5.
EXECUTE HumanResources.uspEmployeesInDepartment 5;
GO
```

Proxies

Create Accounts with special permissions for SQL Server Agent

Proxies

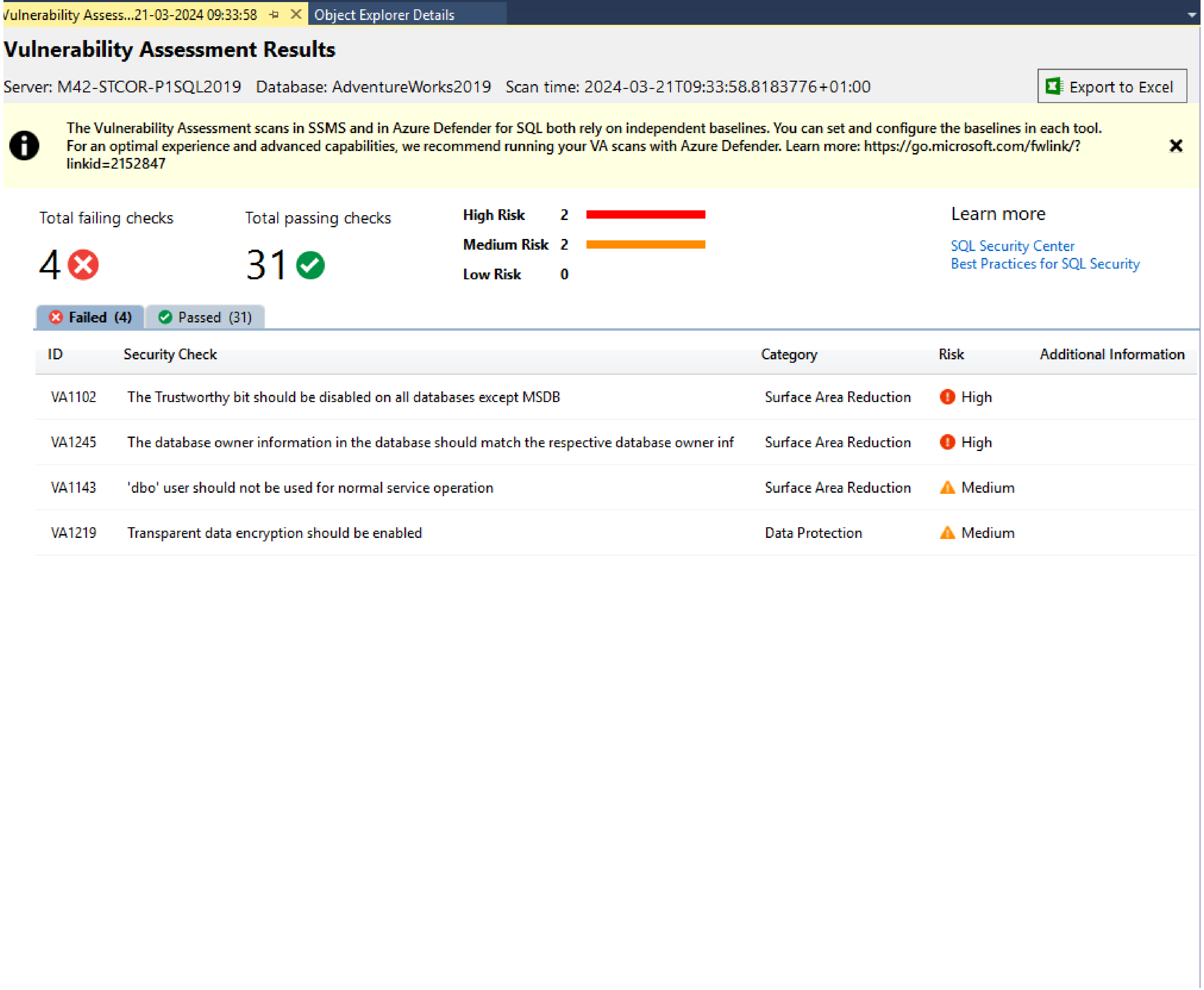
```
-- creates credential CatalogApplicationCredential
USE msdb ;
GO
CREATE CREDENTIAL CatalogApplicationCredential WITH IDENTITY = 'AD-name/DomainUser',
    SECRET = 'lkjhnfalksæhfd$]\';
GO
-- creates proxy "Catalog application proxy" and assigns
-- the credential 'CatAppCred' to it.
EXEC dbo.sp_add_proxy
    @proxy_name = 'Catalog application proxy',
    @enabled = 1,
    @description = 'Maintenance tasks on catalog application.',
    @credential_name = 'CatAppCred' ;
GO
-- grants the proxy "Catalog application proxy" access to
-- the ActiveX Scripting subsystem.
EXEC dbo.sp_grant_proxy_to_subsystem
    @proxy_name = N'Catalog application proxy',
    @subsystem_id = 2 ;
GO

-- subsystem 2-12
-- ActiveX, CmdExec, Snapshot Agent, Log Reader, Distibution Agent, Merge Agent,
-- SSAS Query, SSAS Command, SSIS package execution, PowerShell
```

Vulnerability Assessment

Exists in SSMS 17.4 to 18.12.1 – Free and limited

Not in SSMS 19.X og 20.X

Microsoft Defender for SQL – Not free and unlimited



Vulnerability Assessment Results

Server: M42-STCOR-P1SQL2019 Database: AdventureWorks2019 Scan time: 2024-03-21T09:33:58.8183776+01:00

The Vulnerability Assessment scans in SSMS and in Azure Defender for SQL both rely on independent baselines. You can set and configure the baselines in each tool. For an optimal experience and advanced capabilities, we recommend running your VA scans with Azure Defender. Learn more: https://go.microsoft.com/fwlink/?linkid=2152847

Total failing checks 4 ✗

Total passing checks 31 ✓

High Risk	**2**	🟥
Medium Risk	**2**	🟧
Low Risk	**0**	

ID	Security Check	Category	Risk	Additional Information
VA1102	The Trustworthy bit should be disabled on all databases except MSDB	Surface Area Reduction	! High	
VA1245	The database owner information in the database should match the respective database owner inf	Surface Area Reduction	! High	
VA1143	'dbo' user should not be used for normal service operation	Surface Area Reduction	⚠ Medium	
VA1219	Transparent data encryption should be enabled	Data Protection	⚠ Medium	

Extended Events

xEvents mainly for performance but can be used for security as well

xEvent

```
CREATE EVENT SESSION [audit_tsql] ON SERVER
ADD EVENT sqlserver.existing_connection(
    ACTION(package0.event_sequence,sqlserver.session_id)),
-- Only session_id greater than 50 - exclude internal sessions
ADD EVENT sqlserver.login(SET collect_options_text=(1)
    ACTION(package0.event_sequence,sqlserver.session_id)),
ADD EVENT sqlserver.logout(
    ACTION(package0.event_sequence,sqlserver.session_id)),
ADD EVENT sqlserver.sql_statement_completed(

ACTION(sqlos.task_time,sqlserver.client_hostname,sqlserver.database_name,sqlserver.nt_username,sqlserver
.session_id,sqlserver.sql_text,sqlserver.username)
-- Contains hostname, database, username, text of sql statement
    WHERE ([sqlserver].[session_id]>(50)))
ADD TARGET package0.event_file(SET filename=N'C:\Temp\audit_tsql.xel'),-- When is event file place -
file will contain a timestamp
ADD TARGET package0.ring_buffer(SET max_events_limit=(0),max_memory=(102400))
WITH (MAX_MEMORY=8192 KB,EVENT_RETENTION_MODE=ALLOW_SINGLE_EVENT_LOSS,MAX_DISPATCH_LATENCY=5
SECONDS,MAX_EVENT_SIZE=0 KB,MEMORY_PARTITION_MODE=NONE,TRACK_CAUSALITY=ON,STARTUP_STATE=OFF)
GO
```

Let’s build today’s and tomorrow’s IT. Together?

Thank you for your attention

Steen Cornelius

stcor@itm8.com

Tlf. +45 5139 3147