

# Defending Your SQL Server

## Practical Strategies Against Ransomware

Jeff Iannucci

# Download all slides and scripts



<https://github.com/desertdba/Presentations>

# Who in the world is Jeff Iannucci?



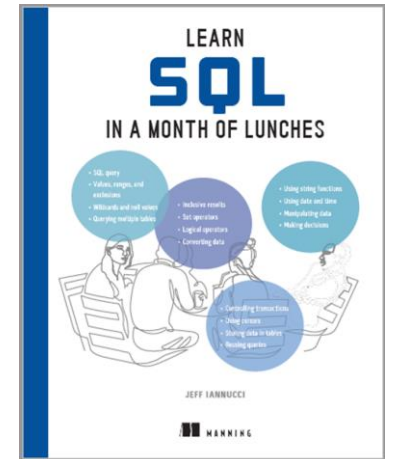
Consultant at Straight Path Solutions



Content Author at Pluralsight



Author of “Learn SQL in a Month of Lunches”



# We made sp\_CheckSecurity!

	VulnerabilityLevel	Vulnerability	Issue	DatabaseName	Details	ActionStep	ReadMoreURL
1	0	Information only	SQL Server name and version	NULL	NC-PRODSQL-SV2\default instance), SQL Server 201...	(Information captured on 04/07/2024)	
2	0	Information only	Communication protocol	NULL	The instance is using the TCP communication protocol ...	If using the TCP protocol, port 1433 is the default.	
3	0	Information only	Remote admin connections	NULL	Remote admin connections are currently ENABLED.	We recommend 'remote admin connections' be ENABLE...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
4	0	Information only	SQL Agent service account	NULL	The SQL Agent service is running with the following ac...	We recommend using managed service accounts if possi...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
5	0	Information only	SQL Server service account	NULL	The SQL Server service is running with the following ac...	We recommend using managed service accounts if possi...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
6	0	Information only	Unencrypted database	NULL	This instance has 13 unencrypted databases.	Having unencrypted databases isn't necessarily bad, but...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
7	1	High - action required	Password is same as login	NULL	Login [adsuser] has a password that is the same as the l...	Change the password to something more secure. Logins...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
8	2	High - review required	clr enabled	NULL	Having the 'clr enabled' setting enabled allows for the e...	Starting with SQL Server 2017, use the configuration opt...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
9	2	High - review required	Failed logins	NULL	There have been at least 2 failed logins recently.	Review the SQL Server error log for patterns of login fail...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
10	2	High - review required	Public permissions	ADSMaster	The [public] role has been granted the permission [CRE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
11	2	High - review required	Public permissions	ADSMaster	The [public] role has been granted the permission [CRE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
12	2	High - review required	Public permissions	ADSMaster	The [public] role has been granted the permission [CRE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
13	2	High - review required	Public permissions	ADSMaster	The [public] role has been granted the permission [CRE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
14	2	High - review required	Public permissions	ADSMaster	The [public] role has been granted the permission [CRE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
15	2	High - review required	Public permissions	ADSMaster	The [public] role has been granted the permission [CRE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
16	2	High - review required	Public permissions	SSISDB	The [public] role has been granted the permission [EXE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
17	2	High - review required	Public permissions	SSISDB	The [public] role has been granted the permission [EXE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
18	2	High - review required	Public permissions	SSISDB	The [public] role has been granted the permission [EXE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
19	2	High - review required	Public permissions	SSISDB	The [public] role has been granted the permission [EXE...	Because these permissions are available to anyone who...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>
20	2	High - review required	sysadmin role members	NULL	Login [ADSCORP\Administrator] is a sysadmin. They ca...	Review the list of logins and groups in the sysadmin role ...	<a href="https://straightpathsql.com">https://straightpathsql.com</a>

[https://github.com/Straight-Path-Solutions/sp\\_CheckSecurity](https://github.com/Straight-Path-Solutions/sp_CheckSecurity)





























# What are we discussing today?

What exactly is ransomware?

Where are your biggest SQL Server vulnerabilities?

How can you prepare for ransomware?



# What are we NOT discussing today?

## Other cyber attacks

- Other malware
- Denial of Service (DoS)

## Other data breaches

- Stolen data
- Publicly available data

# Why should you care about ransomware?

According to the Verizon 2023 Data Breach Investigations Report (DBIR) ransomware attacks were involved in 24% of all breaches.

Ransomware affected 66% of organizations in 2023, according to Sophos' "The State of Ransomware 2023" report.

Since 2020, there have been more than 130 different ransomware strains detected, according to VirusTotal's "Ransomware in a Global Context" report.

<https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>



# What is ransomware?

And what happened to your eggs?



# What happens with a ransomware attack?

## Access

- Phishing
- SQL Server

## Infection

- Scanning
- Escalate privileges
- Malware installation

## Encryption

## Ransom demand





# Options for responding to ransomware

## Pay the ransom

- Typically paid by insurance
- May or may not provide the decryption key
- Could take days/weeks to recover all files..if ever

## Ignore the ransomware demand

- Completely rebuild your environment somewhere else
- Restore all your data from the last available recovery point in time

## Go out of business

- ˘\\_(\ツ)\\_/˘



# You can pay the ransom, but...

“Recent data from Rubrik Zero Labs has found that of all the organizations that suffered a ransomware attack and paid for the decryptor, just 16% actually managed to recover all of their data.”

<https://www.techradar.com/news/microsoft-sql-servers-hacked-to-spread-ransomware>

## SQL Server?

“The researchers note that the ransomware infection starts with the MS-SQL process on the compromised machine downloading a .NET file using cmd.exe and powershell.exe.”

### Microsoft SQL servers hacked in TargetCompany ransomware attacks

By Bill Toulas

September 24, 2022 11:12 AM 1



Vulnerable Microsoft SQL servers are being targeted in a new wave of attacks with FARGO ransomware, security researchers are warning.

<https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-in-targetcompany-ransomware-attacks/>

## SQL Server?

“Once they gain access to the endpoint, the attackers will first install a piece of malware the researchers named CLR Shell. This malware picks up system information, changes the compromised account’s configuration, and escalates privileges to LocalSystem through a vulnerability in the Windows Secondary Logon Service.”

<https://www.techradar.com/news/microsoft-sql-servers-hacked-to-spread-ransomware>

## Microsoft SQL servers hacked to spread ransomware

News

By Sead Fadilpašić published April 20, 2023

Hackers are after poorly configured Microsoft SQL servers





## SQL Server?

“The attacks start with threat actors scanning for servers with an open TCP port 1433, which are likely public-facing MS-SQL servers. The attacker then carries out brute-forcing and dictionary attacks to crack the password. For the attack to work with either method, the target password has to be weak.”

<https://www.bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/>

## Vulnerable Microsoft SQL Servers targeted with Cobalt Strike

By **Bill Toulas**

February 22, 2022 01:08 PM 0



Threat analysts have observed a new wave of attacks installing Cobalt Strike beacons on vulnerable Microsoft SQL Servers, leading to deeper infiltration and subsequent malware infections.

# What are SQL Server's vulnerabilities?

So many vulnerabilities.





But first...principles!

Just two.





# Principle of Zero Trust

## Verify explicitly

- Always authenticate and authorize based on all available data points.

## Assume breach

- Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

<https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview>

# Principle of Least Privilege

Grant users account or processes only those privileges which are essentially vital to perform its intended functions.

- Database roles
- Instance roles
- Server roles

“Know your role...” – Dwayne “The Rock” Johnson

[https://en.wikipedia.org/wiki/Principle\\_of\\_least\\_privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege)



# Login vulnerabilities

It starts with access.



## The sa login is enabled

Every instance has/needs sa  
...and it's in the sysadmin role  
Most common attack point  
Disabling = no connections  
Can still use sa when disabled

```
/* check to see if sa is disabled */  
SELECT
```

```
    name
```

```
    , is_disabled
```

```
FROM sys.server_principals
```

```
WHERE sid = 0x01;
```

```
/* disabled sa */
```

```
ALTER LOGIN [sa] DISABLE;
```



# sysadmin role members

Members of sysadmin can do  
anything in SQL Server

Review current sysadmins

Avoid SQL Server logins

```
/* find members of sysadmin role */  
SELECT  
    name  
    ,type_desc  
    ,is_disabled  
FROM sys.server_principals  
WHERE IS_SRVROLEMEMBER ('sysadmin',name) = 1  
ORDER BY name
```

# CONTROL SERVER permissions

Virtually identical to sysadmin  
permissions

Can impersonate sysadmin  
members

Often unnoticed

Why are you using this?

```
/* find logins with CONTROL SERVER */  
SELECT  
    name  
    ,type_desc  
    ,is_disabled  
FROM sys.server_principals AS pri  
WHERE pri.[principal_id] IN (  
    SELECT p.[grantee_principal_id]  
    FROM sys.server_permissions AS p  
    WHERE p.[state] IN ( 'G', 'W' )  
    AND p.[class] = 100  
    AND p.[type] = 'CL'  
    )  
AND pri.[name] NOT LIKE '###%###';
```



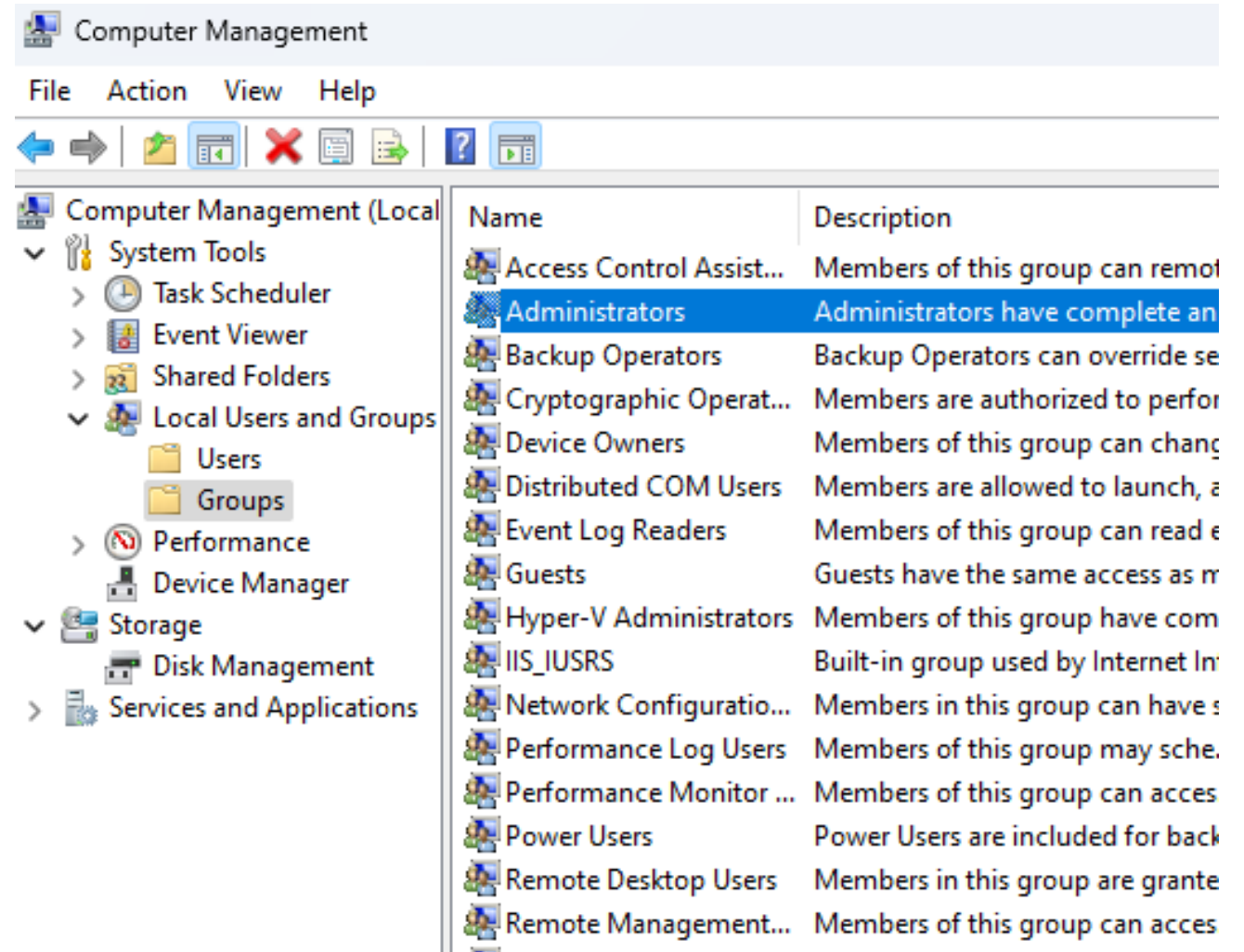
# Local Administrators group members

Windows group

May already be in sysadmin role

Can add themselves to sysadmin role

<https://straightpathsql.com/archives/2023/08/adding-sql-server-access-when-youre-locked-out/>



# Password issues

Password is blank

Password is same as the login

Password is “password”

Yes, you can find these!

```
/* blank passwords */  
SELECT name  
FROM sys.sql_logins  
WHERE PWDCOMPARE('',password_hash)=1;
```

```
/* password same as login */  
SELECT name  
FROM sys.sql_logins  
WHERE PWDCOMPARE(name,password_hash)=1;
```

```
/* passwords is password */  
SELECT name  
FROM sys.sql_logins  
WHERE PWDCOMPARE('password',password_hash)=1;
```

# SQL Server logins

No MFA

Not identity specific

Limit permissions for logins

Create “secure” passwords





# What is a “secure” password?

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

<https://tech.co/password-managers/how-long-hacker-crack-password>

# Instance vulnerabilities

Have you been taking care of  
your SQL Server?



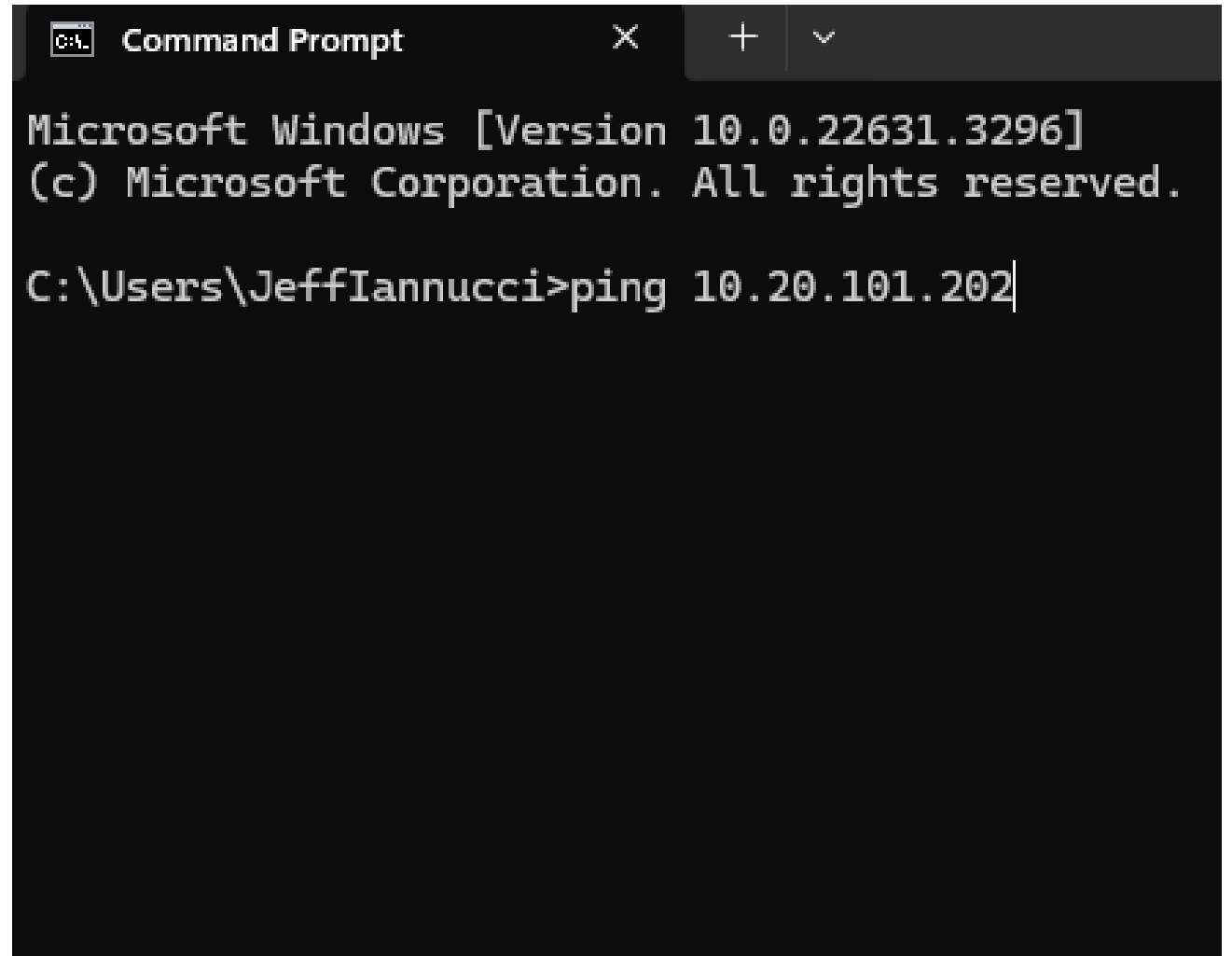
# Is your SQL Server public facing?

Should it be?

Is your firewall configured?

Do you know your IP?

Can you ping your server?

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The window content shows the following text: "Microsoft Windows [Version 10.0.22631.3296] (c) Microsoft Corporation. All rights reserved. C:\Users\JeffIannucci>ping 10.20.101.202". The cursor is at the end of the command line.

```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\JeffIannucci>ping 10.20.101.202
```



# Cumulative updates

Contain vulnerability fixes

Apply GDRs too

Who do you think knows about these vulnerabilities?

Create an update schedule

<https://sqlserverupdates.com>

## What are the most recent updates for SQL Server?

Here are the most recent service packs and cumulative updates for SQL Server, and [here's how to patch your server](#):

Version	Latest Update	Build Number	Support Ends	Other Updates
SSMS 20	<a href="#">Download Most Recent</a>			<a href="#">SSMS 17 w/Debugger</a>
Azure Data Studio	<a href="#">Download Most Recent</a>			
SQL Server 2022	<a href="#">Download RTM</a> then <a href="#">CU12</a> then <a href="#">GDR</a>	16.0.4120.1	2033/01/11	<a href="#">Other SQL 2022 Updates</a>
SQL Server 2019	<a href="#">Download RTM</a> then <a href="#">CU25</a> then <a href="#">GDR</a>	15.0.4360.2	2030/01/08	<a href="#">Other SQL 2019 Updates</a>
SQL Server 2017	<a href="#">Download RTM</a> then <a href="#">CU31</a> then <a href="#">GDR</a>	14.0.3465.1	2027/10/12	<a href="#">Other SQL 2017 Updates</a>
SQL Server 2016	<a href="#">Download RTM (or Developer)</a> then <a href="#">SP3</a> then <a href="#">GDR</a>	13.0.6435.1	2026/07/14	<a href="#">Other SQL 2016 Updates</a>
SQL Server 2014	<a href="#">Download SP3</a> then <a href="#">CU4</a> then <a href="#">GDR</a>	12.0.6449.1	2024/07/09	<a href="#">Other SQL 2014 Updates</a>
SQL Server 2012	<a href="#">Download SP4</a> then <a href="#">GDR</a>	11.0.7512.11	2022/07/12	<a href="#">Other SQL 2012 Updates</a>

## SQL Login Audit doesn't include failed logins

This is NOT the default

Auditing failed logins can reveal hacking attempts

...and more!

Check your SQL Server logs

**sp\_readerrorlog**

Server authentication

- ☐ Windows Authentication mode
- ☒ SQL Server and Windows Authentication mode

Login auditing

- ☐ None
- ☒ Failed logins only
- ☐ Successful logins only
- ☐ Both failed and successful logins

Server proxy account

☐ Enable server proxy account

Proxy account:

Password:

Options

## Linked servers

What security context?

PLEASE NOT sa!

...or another sysadmin!

Local server login to remote server login mappings:

Local Login	Impersonate	Remote User	Remote Password
-------------	-------------	-------------	-----------------

For a login not defined in the list above, connections will:

☐ Not be made

☐ Be made without using a security context

☐ Be made using the login's current security context

☒ Be made using this security context:

Remote login:

With password:



## CLR enabled

This is NOT a default  
Allows user assembly  
execution

Why not T-SQL?

2017+? Use 'clr strict security'

```
/* is CLR enabled? */
```

```
SELECT *
```

```
FROM master.sys.configurations 1
```

```
WHERE [name] = 'clr enabled';
```

```
/* is strict CLR enabled? */
```

```
SELECT *
```

```
FROM master.sys.configurations 1
```

```
WHERE [name] = 'clr strict security';
```

## xp\_cmdshell enabled

This is NOT a default

Shell for external commands

Only members of sysadmin  
can use

Only members of sysadmin  
can enable

The real issue: Who is a  
sysadmin?

```
/* is xp_cmdshell enabled? */  
SELECT *  
FROM master.sys.configurations  
WHERE [name] = 'xp_cmdshell';
```

# Backup vulnerabilities

Have you been taking care of your eggs?





# Do you have database backups

Native backups are great!

Enable compression,  
checksum

VM backups do not count!

Is your backup software  
application-aware?

System databases?

Offsite?

Have you tested restoring?

```
/* Check for full backups */
SELECT
    s.server_name AS InstanceName
    , s.database_name AS DatabaseName
    , s.recovery_model AS RecoveryModel
    , s.is_copy_only
    , s.is_snapshot
    , s.has_backup_checksums
    , s.backup_start_date AS BackupStartDate
    , s.backup_finish_date AS BackupFinishDate
    , CAST(DATEDIFF(second, s.backup_start_date, s.backup_finish_date) AS VARCHAR(4))
      + ' ' + 'Seconds' AS Duration
    , CAST(CAST(s.backup_size / 1000000 AS INT) AS VARCHAR(14)) + ' ' + 'MB' AS SizeInMB
    , m.physical_device_name AS PhysicalDevice
    , m.logical_device_name AS LogicalDevice
    , CASE m.device_type
        WHEN 2 THEN 'Disk'
        WHEN 5 THEN 'Tape'
        WHEN 7 THEN 'Virtual Device'
        WHEN 9 THEN 'Azure Storage'
        WHEN 2 THEN 'A permanent Backup Device'
        ELSE 'UNKNOWN'
    END AS DeviceType
    , s.[user_name] AS UserName
FROM msdb.dbo.backupset s
INNER JOIN msdb.dbo.backupmediafamily m
    ON s.media_set_id = m.media_set_id
WHERE s.[Type] = 'D' /* Full backups */
ORDER BY s.backup_start_date DESC
```

# Do you have log backups

Native log backups are great!

Compression and checksum help with these too

Is your backup software backing up the log...to NUL?

Have you tested restoring to a point in time?

```
/* Check for log backups */
SELECT
    s.server_name AS InstanceName
  , s.database_name AS DatabaseName
  , s.recovery_model AS RecoveryModel
  , s.is_copy_only
  , s.is_snapshot
  , s.has_backup_checksums
  , s.backup_start_date AS BackupStartDate
  , s.backup_finish_date AS BackupFinishDate
  , CAST(DATEDIFF(second, s.backup_start_date, s.backup_finish_date) AS VARCHAR(4))
    + ' ' + 'Seconds' AS Duration
  , CAST(CAST(s.backup_size / 1000000 AS INT) AS VARCHAR(14)) + ' ' + 'MB' AS SizeInMB
  , m.physical_device_name AS PhysicalDevice
  , m.logical_device_name AS LogicalDevice
  , CASE m.device_type
      WHEN 2 THEN 'Disk'
      WHEN 5 THEN 'Tape'
      WHEN 7 THEN 'Virtual Device'
      WHEN 9 THEN 'Azure Storage'
      WHEN 2 THEN 'A permanent Backup Device'
      ELSE 'UNKNOWN'
    END AS DeviceType
  , s.[user_name] AS UserName
FROM msdb.dbo.backupset s
INNER JOIN msdb.dbo.backupmediafamily m
    ON s.media_set_id = m.media_set_id
WHERE s.[Type] = 'L' /* Log backups */
ORDER BY s.backup_start_date DESC
```

# Is your backup chain consistent?

## Multiple backups in different places

## Do you have copy-only backups?

## ...have you tested restoring?

<https://straightpathsql.com/archives/2023/10/audit-your-database-backup-chain/>

## Audit Your Database Backup Chain!

October 30, 2023 by David Seis

All database administrators know that safeguarding data is paramount and having a strong restore strategy is crucial. In this post, I would like to add another tool to your arsenal that I have found helpful in auditing server health and configurations as it pertains to backups and the backup chain.

A backup chain is important when it comes to recovery. If you have full, diff, and log backups going to different backup locations, non-copy-only off-cycle backups from developers or testers, or other strangeness in your server's backup history, you could be in a world of hurt should you need to restore to a specific time.

The script below will look through msdb and add up the number of each type of backup found and count how many are going to different locations, separated by native to a network share, third party via GUID, or native to a local disk location.

```
1.  /*****
2.  /*#          Created by David Seis          #*/
3.  /*#          4/18/2023                      #*/
4.  /*#          #*/
5.  /*#          Straight Path IT Solutions, LLC. #*/
6.  /*****
7.
8.  /*
9.  Description:
10. - This identifies the number of sql server backups detected in the time period from the backup history log in
    msdb, breaks it down by distinct locations found, how many native share, native local, and third party guid
    backups found. the second result set outputs each found unique backup location per database and backup type.
11.
12. - 4/19/2023 - counting third party tools as 1 location
13. */
14. --
```



# We also made sp\_CheckBackup!

	InstanceName	DatabaseName	AvailabilityGroupName	RecoveryModel	BackupType	BackupSetID	IsCopyOnly	IsSnapshot	IsPasswordProtected	HasBackupChecksum	BackupStartDate	BackupFinishDate
1	LAPTOP-9K06NS8T	Dummy	NULL	Full	Full	23	No	No	No	No	2024-08-01 10:42:38.000	2024-08-01 10:42:38.000
2	LAPTOP-9K06NS8T	Dummy	NULL	Full	Full	22	No	No	No	Yes	2024-07-11 13:23:55.000	2024-07-11 13:23:55.000
3	LAPTOP-9K06NS8T	Dummy	NULL	Full	Transaction Log	21	No	No	No	No	2024-07-11 13:15:59.000	2024-07-11 13:15:59.000
4	LAPTOP-9K06NS8T	Dummy	NULL	Full	Full	20	No	No	No	Yes	2024-07-11 13:13:05.000	2024-07-11 13:13:05.000
5	LAPTOP-9K06NS8T	Dummy	NULL	Full	Full	20	No	No	No	Yes	2024-07-11 13:13:05.000	2024-07-11 13:13:05.000
6	LAPTOP-9K06NS8T	Dummy	NULL	Full	Full	20	No	No	No	Yes	2024-07-11 13:13:05.000	2024-07-11 13:13:05.000
7	LAPTOP-9K06NS8T	Dummy	NULL	Full	Full	20	No	No	No	Yes	2024-07-11 13:13:05.000	2024-07-11 13:13:05.000
8	LAPTOP-9K06NS8T	DB_Administration	NULL	Full	Full	19	No	No	No	No	2024-04-21 10:26:12.000	2024-04-21 10:26:12.000
9	LAPTOP-9K06NS8T	DB_Administration	NULL	Full	Full	14	No	No	No	No	2024-04-21 10:26:11.000	2024-04-21 10:26:11.000
10	LAPTOP-9K06NS8T	DB_Administration	NULL	Full	Full	15	No	No	No	No	2024-04-21 10:26:11.000	2024-04-21 10:26:11.000
11	LAPTOP-9K06NS8T	DB_Administration	NULL	Full	Full	16	No	No	No	No	2024-04-21 10:26:11.000	2024-04-21 10:26:11.000
12	LAPTOP-9K06NS8T	DB_Administration	NULL	Full	Full	17	No	No	No	No	2024-04-21 10:26:11.000	2024-04-21 10:26:11.000
13	LAPTOP-9K06NS8T	DB_Administration	NULL	Full	Full	18	No	No	No	No	2024-04-21 10:26:11.000	2024-04-21 10:26:12.000
14	LAPTOP-9K06NS8T	master	NULL	Simple	Full	11	No	No	No	Yes	2024-04-21 09:05:13.000	2024-04-21 09:05:13.000
15	LAPTOP-9K06NS8T	model	NULL	Full	Full	12	No	No	No	Yes	2024-04-21 09:05:13.000	2024-04-21 09:05:13.000
16	LAPTOP-9K06NS8T	msdb	NULL	Simple	Full	13	No	No	No	Yes	2024-04-21 09:05:13.000	2024-04-21 09:05:13.000
17	LAPTOP-9K06NS8T	master	NULL	Simple	Full	8	No	No	No	Yes	2024-04-21 08:17:00.000	2024-04-21 08:17:00.000
18	LAPTOP-9K06NS8T	model	NULL	Full	Full	9	No	No	No	Yes	2024-04-21 08:17:00.000	2024-04-21 08:17:00.000
19	LAPTOP-9K06NS8T	msdb	NULL	Simple	Full	10	No	No	No	Yes	2024-04-21 08:17:00.000	2024-04-21 08:17:01.000
20	LAPTOP-9K06NS8T	DB_Administration	NULL	Full	Transaction Log	7	No	No	No	Yes	2024-04-19 19:48:28.000	2024-04-19 19:48:28.000

[https://github.com/Straight-Path-Solutions/sp\\_CheckBackup](https://github.com/Straight-Path-Solutions/sp_CheckBackup)

## How can you prepare?

In so far as it depends on you...protect the nest with this [checklist](#) of Action Items!



# 1. Identify all instances

## Document all your instances

- Server and instance name
- Communication protocols and ports used
- Resources assigned including drives
- IP addresses

Are they external facing?

Did you find them all?

- Find-DbalInstance
- <https://docs.dbatools.io/Find-DbalInstance.html>



## 2. Review your instances

### Apply Cumulative Updates and GDRs

- <https://sqlserverupdates.com/>
- Develop a schedule

### Check your linked servers

### Check for CLR usage

- If possible, disable
- If necessary, use clr strict security

### Capture failed login attempts

# 3. Review failed logins

## Review the SQL Server log

- Check the IP addresses
- Use Extended Events of SQL Server Audit for more info

## sp\_readerrorlog

- <https://learn.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-readerrorlog-transact-sql?view=sql-server-ver16>
- SQL Agent job?

## 4. Limit SQL Server permissions

### Disable the sa login

#### Check for password vulnerabilities

- Blank
- Same as login
- “password”

#### Principle of Least Privilege (a.k.a. Know your role!)

- sysadmin role?
- local Administrators group?
- CONTROL SERVER?

Are there any SQL Server logins with these permissions?



## 5. Use strong passwords for SQL Server logins

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

<https://tech.co/password-managers/how-long-hacker-crack-password>

## 6. Verify your schedule of backups

Do you have database backups?

- How often?
- Is the backup chain broken?

Do you have log backups?

- How often?
- Are they to NUL?

Do you have backups of encryption keys and certificates?

Are your backups offsite?

What is your Recovery Point Objective (RPO)?

## 7. Test “recover from zero”

Assume a breach has occurred or will occur

Have you restored...

- A database from a backup?
- Your **largest** database from backup?
- An entire server from backup?
- Multiple servers from backup?

How long do these operations this take?

What is your Recovery Time Objective (RTO)?



## 8. Check with your colleagues

### Principle of Zero Trust

#### Your systems & network administrators

- Use Antivirus software according to Microsoft recommendations
- <https://learn.microsoft.com/en-us/troubleshoot/sql/database-engine/security/antivirus-and-sql-server>
- Use MFA

#### Stop clicking on stupid emails and attachments

- Haha! Right?
- Seriously though, Phishing is the most common entry point for ransomware

# You have Action Items!

Go, do all the things to  
prevent and prepare!



# Ransomware is inevitable

“...Ransomware affected 66% of all organizations in 2023...”

“...Just 16% managed to recover all their data...”

# Be Prepared!



<https://github.com/desertdba/Presentations>



[www.linkedin.com/in/jeff-iannucci](https://www.linkedin.com/in/jeff-iannucci)



[https://github.com/Straight-Path-Solutions/sp\\_CheckSecurity](https://github.com/Straight-Path-Solutions/sp_CheckSecurity)

[https://github.com/Straight-Path-Solutions/sp\\_CheckBackup](https://github.com/Straight-Path-Solutions/sp_CheckBackup)

