

4N6 Cyber Resilience Internship

ASSIGNMENT(Set-2)

Penetration Testing Report – Security Control Auditing:

Web application security is a key concern for any organization. The software security community created the Open Web Application Security Project (OWASP) to help educate developers and security professionals. This report provides Tenable.sc users the ability to monitor web applications by identifying the top 10 most critical vulnerabilities as described in OWASP's Top 10 awareness document.

The OWASP Top 10 outlines several different aspects of web based security, from Cross-Site scripting attacks, Security Misconfigurations, and Sensitive data exposure. The Top 10's focus is to reduce risk across the most vulnerable aspects of conducting business across the internet. Following these guidelines empowers organizations to reduce risk to organizational and customer data theft.

Administrators need to ensure that their organization isn't vulnerable to any of the attacks that relate to the 10 different focuses of the Top 10. In addition, the compliance related focuses, like the known vulnerable components and insufficient logging, are important for eliminating gaps in an organization's security that aren't directly tied to exploitable attacks.

This report covers all aspects of the OWASP Top 10, and gives administrators the tools and information needed to aid their efforts. The chapters related to exploitable vulnerabilities gives organizations a roadmap for reducing attack risk. The compliance and logging chapters will also guide organizations on the steps that they need to take to mitigate business risk through strong security practice.

The report is available in the SecurityCenter Feed, a comprehensive collection of dashboards, reports, assurance report cards and assets. The report can be easily located in the SecurityCenter Feed under the category Security Industry Trends. The report requirements are:

- Tenable.sc 5.2.0
- Nessus 8.4.0

Nikhil Yadav (nikhil27rock@gmail.com)

- LCE 6.0.0
- NNM 5.9.0

Tenable.sc CV provides continuous network monitoring, vulnerability identification, risk reduction, and compliance monitoring. Nessus is continuously updated with information about advanced threats and zero-day vulnerabilities, and new types of regulatory compliance configuration audits. By integrating with Nessus, Tenable.sc CV provides the most comprehensive view of network security data.

Executive Summary - This chapter is comprised of seven components, starting with two 90-day trend graphs, depicting critical and high severity vulnerabilities discovered over the past six months. There are two indicator components that monitor web server, SQL Server, and IDS logs for web application events. The third indicator component provides a view into several web application security issues starting with injection vulnerabilities and ending with cross-site scripting (XSS) vulnerabilities. There is a table with all informational vulnerabilities related to web application security. The final component is a detailed matrix showing vulnerabilities mapped to the ten most critical web application security risks identified in OWASP's Top Ten document. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Top 10 Security Flaws Details - This chapter covers in detail the 10 most common security flaws identified in the OWASP Top 10. The chapter is broken down into a section for each security flaw, and contains a pie chart and vulnerability summary table.

PCI DSS Requirement 6.5 Common Coding Flaws - This chapter reviews the requirements in PCI DSS requirement 6.5. The requirement addresses many of the security flaws found in the OWASP Top 10. The chapter is broken down into a section for each security flaw, and contains a pie chart and vulnerability summary table.

OWASP Web Events - This chapter contains events collected by NNM and web applications, and can be used to analyze the security of web applications. The chapter is broken into several sections and contain network summary pie chart, list of normalized events, followed by a top 100 IP address summary.

OWASP SQL Events - This chapter contains events collected by Database and SQL applications, and can be used to analyze the security of web applications. The chapter is broken into several sections and contain network summary pie chart, list of normalized events, followed by a top 100 IP address summary.

Nikhil Yadav (nikhil27rock@gmail.com)

Introducing Open-Audit

Open-Audit is an application to tell you exactly **what** is on your network, **how** it is configured and **when** it changes. Open-Audit will run on Windows and Linux systems. Essentially, Open-Audit is a database of information, that can be queried via a web interface. Data about the network is inserted via a Bash Script (Linux) or VBScript (Windows). The entire application is written in php, bash and vbscript. These are all 'scripting' languages - no compiling and human readable source code. Making changes and customisations is both quick and easy.

Windows PCs can be queried for hardware, software, operating system settings, security settings, IIS settings, services, users & groups and much more. Linux systems can be queried for a similar amount of information. Network devices (printers, switches, routers, etc) can have data recorded such as IP-Address, MAC Address, open ports, serial number, etc, etc. Output is available in PDF, CSV and webpages. There are export options for Dia and Inkscape.

Open-Audit can be configured to scan your network and devices automatically. A daily scan is recommended for systems, with network scans every couple of hours. That way, you can be assured of being notified if something changes (day to day) on a PC, or even sooner, if something "new" appears on your network.

Nsauditor Network Security Auditor

Nsauditor Network Security Auditor - Advanced All-In-One Network Security Auditing Tools Suite, includes more than 45 network tools and utilities for network security auditing, network scanning, network monitoring and more.

Network Auditor is a tool to discover the network services and to check them for discovering well known vulnerabilities. This tool creates an audit report. The auditor consists in two main parts: TCP and UDP. To enable an option (options) select appropriate checkboxes.

The enabled Extended Tcp Ports (Extended Udp Ports) feature contains the number of ports, used to audit the network. You can add ports by clicking on the Add Ports button and selecting port from [Ports Dialog](#).

Network Audit Dialog

☒ **TCP**

☒ **Extended Tcp Ports**
 Ports (Example: 13,17,21-23,25,42,43,53,79-80,109-111,113,118-119,135,137-139,143)
 13,17,21-23,25,42,43,53,79-80,109-111,113,118-119,135,137-139,143,156,179,389,443,445,512-515, Add Ports

☒ **Ftp Vulnerabilities (Port 21)**
☒ Check Ftp Vulnerabilities
☐ Check Weak Passwords

☒ **Telnet Vulnerabilities (Port 23)**
☒ Check Telnet Vulnerabilities
☐ Check Weak Passwords

☒ **Tcp Services**
☒ Who Is (Port 43)
☒ Finger (Port 79)
☒ Sun Rpc (Port 111)
☒ Ms Rpc (Port 135)
☒ IMAP4 (Port 143)
☒ Remote EXEC (Port 512)
☒ Ms SQL (Port 1433)
☒ My SQL (Port 3306)
☒ Plug and Play (Port 5000)

☒ **Sntp Vulnerabilities (Port 25)**
☒ SMTP Vulnerabilities
☒ SMTP Relaying

☒ **Pop3 Vulnerabilities (Port 110)**
☒ Check Pop Vulnerabilities
☐ Check Weak Passwords

☒ **Http Vulnerabilities (Port 80,8080)**
 Common
 Apache
 Netscape
 ColdFusion
 Frontpage
 IIS

☒ **Net Bios**
☒ NetBios Names, Common Info
☒ Retrieve Users Logs
☒ Enumerate Users
☒ Enumerate Machines
☒ Enumerate Groups
☒ Enumerate Shares
☒ Enumerate Hidden Shares
☒ Enumerate Connections
☒ Enumerate Network Devices
☒ Enumerate Services
☒ Enumerate Processes
☒ Retrieve Policies Information
☒ Retrieve Registry Information
☒ Retrieve Time of Day
☐ Check Weak Passwords

☒ **Udp**

☒ **Extended Udp Ports**
 Ports (Example: 42,43,53,67-69,88,111,135-138,143,161,445,514,520,1900)
 42,43,53,67-69,88,138,143,445,514,520,1433,1512 Add Ports

☒ **Udp Services**
☒ Ms Rpc (Port 135)
☒ Sun Rpc (Port 111)
☒ NetBios Name (Port 137)
☒ Snmp Vulnerabilities (Port 161)
☒ MsSql Monitor (Port 1434)
☒ Plug and Play (Port 1900)

Target Host / Local Interface / Command Buttons

Profile Name: Timeout:

Local Interface:

Target Host:

Scan Mode: ☒ Connect ☐ SYN

Report Mode: ☒ Html ☐ Xml

Load Default Load Profile Save Profile

Start Audit Cancel Save As

To audit ftp vulnerabilities enable **Ftp Vulnerabilities** option. This option allows you to check **Ftp Vulnerabilities** and **Weak Passords** . To audit smtp vulnerabilities enable Sntp Vulnerabilities option.

This option allows you to check **SMTP Vulnerabilities** and **SMTP Relaying**. To audit telnet vulnerabilities enable **Telnet Vulnerabilities** option. This option allows you to check **Telnet Vulnerabilities** and **Weak Passwords** . To audit pop3 vulnerabilities enable **Pop3 Vulnerabilities** option. This option allows you to check **Pop Vulnerabilities** and **Weak Passwords**.

To audit different Net Bios settings you can enable some or all **Net Bios** options including **NetBios Names, User Logs, Users, etc.**

To audit different **Tcp** services you can enable some or all **Tcp Services** including **Who Is, Finger, etc.**

To audit http vulnerabilities enable **Http Vulnerabilities** option.

To audit different **Udp** services you can enable some or all **Udp Services** including **Dns Vulnerabilities, Sun Rpc, Snmp Vulnerabilities , Plug and Play Vulnerabilities, MsSql Monitor.**

Nikhil Yadav (nikhil27rock@gmail.com)

You can change scan mode from Connect to **SYN**. You can also select one of the following report modes

XML or HTML.

The field **Profile Name** contains the profile name. The profile can be loaded by clicking on the **Load Profile** button and selecting the file name (The profile file is stored in XML format).

Clicking on the **Load Default** button loads the default profile. Clicking on the **Save Profile** button will save the profile in the selected file. You can save the profile in another file by clicking on the **Save As** button.

To start auditing clicking on the **Start Audit** button .

To close the dialog click on the **Cancel** button.

To load an interface click on the **Local** Interface button. **Clicking** on this button opens the

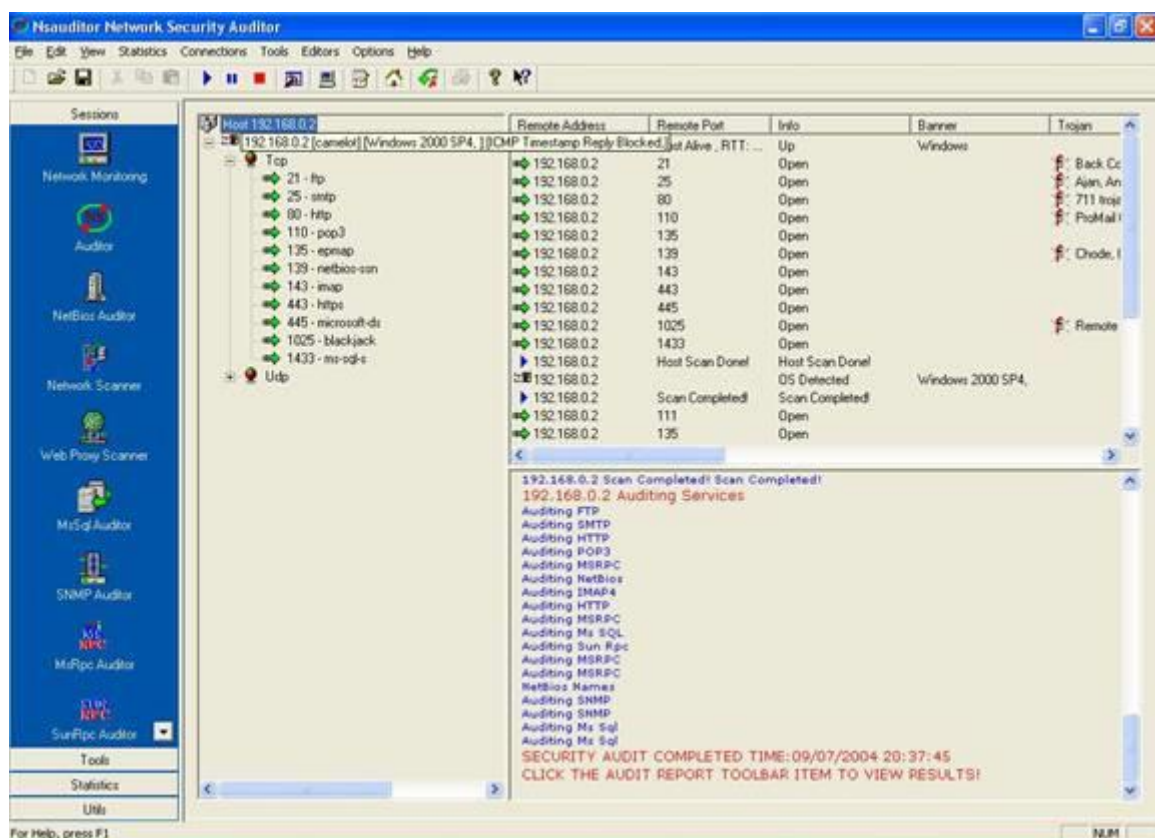
[AVAILABLE NETWORK INTERFACES](#) dialog.

Clicking on the button **Target** Host opens the [Host Range and Credentials Selection Dialog](#).

After the auditing process is started the **Network Audit Dialog** will be closed and the view that shows

the audit process will appear in the screen.

The left part of the view contains all selected **TCP** and **UDP** ports. The top of the right part contains the remote host settings including **Remote Address, Remote Port , Info, Banner, Trojan, Service Name, Service Description**. The bottom of the right part contains information about the current auditing process.



This section provides you with information about the reports that are available by default in the **Reports** tab of GFI LanGuard.

There are two main types of reports:

- **General reports** - provide detailed technical reports as well as executive summary reports about LAN security and patch management activity
- **Legal compliance reports** - provide system and network audit information that enable you to be compliant with standards, laws and regulations related to corporate network usage and management conventions.

General reports

To view **General** reports:

1. Click **Reports** tab.
2. Click **View**, and from the list of reports, click **General Reports**, then select any of the following reports:

Report Title	Description
Network Security Overview	An executive summary report showing: <ul style="list-style-type: none">• Network vulnerability level• Most vulnerable computers• Agent status• Audit status• Vulnerability trends over time• Information on operating systems• Servers and workstations.
Computer Security Overview	An executive summary report showing: <ul style="list-style-type: none">• Computer vulnerability level• Agent status• Audit status• Vulnerability trends over time• Computer summary and details.
Vulnerability Status	Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by: <ul style="list-style-type: none">• Computer name• Vulnerability severity• Timestamp• Category.
Patching Status	Shows statistical information related to missing and installed updates detected on your scan targets. Updates can be grouped by name, severity, timestamp, vendor and category. Use this report to get: <ul style="list-style-type: none">• Missing vs. Installed updates comparison• Charts and tables displaying missing updates distribution for each item from the first and second grouping criteria• Charts and tables displaying installed updates distribution for each item from the first and second grouping criteria• Patching details for missing and installed patches.

Report Title	Description
Full Audit	<p>A technical report showing information retrieved during an audit. Amongst others, the report contains information on:</p> <ul style="list-style-type: none"> • Vulnerabilities • Open ports • Hardware and software.
Software Audit	<p>Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on:</p> <ul style="list-style-type: none"> • Antivirus • Antispyware • Applications inventory.
Scan History	<p>An overview of the network security audits performed over time. Amongst others, the report includes information on:</p> <ul style="list-style-type: none"> • Most scanned computers • Least scanned computers • Auditing status • History listing.
Remediation History	<p>Shows information related to remediation actions performed on target computers. Amongst others, the report includes information on:</p> <ul style="list-style-type: none"> • Remediation actions per day • Remediation distribution by category • Remediation list grouped by computers.
Network Security History	<p>Shows the changes done on scan targets between audits. Amongst others, the report includes changes related to:</p> <ul style="list-style-type: none"> • The vulnerability level • User accounts • Groups • Ports • Shares • Registry entries.
Baseline Comparison	<p>Enables you to compare the results of all scan targets to a base computer. From the drop down list select the base computers and click Generate. The results are grouped by computer name and amongst others includes information on:</p> <ul style="list-style-type: none"> • Registry • Installed Service Packs and Update Rollups • Missing Security/Non-Security Updates • Vulnerability level.
Mobile Devices Audit	<p>Shows information related to detected mobile devices found during an audit. Amongst others, the report includes information on:</p> <ul style="list-style-type: none"> • Vulnerability distribution by severity • Vulnerability distribution by computer • Vulnerability listing by computer.

Report Title	Description
USB Devices	Lists all USB devices found in an audit, grouped by computer.
Missing Microsoft® Security Updates	Shows statistical information related to missing Microsoft® security updates, detected on your scan targets. Select items to include in your report: <ul style="list-style-type: none"> • General missing updates distribution chart • Distribution table • Vulnerability list.
Missing Non-Microsoft® Security Updates	Shows statistical information related to missing non-Microsoft® security updates, detected on your scan targets. Select items to include in your report: <ul style="list-style-type: none"> • General missing updates distribution chart • Distribution table • Vulnerability list.
Missing Security Updates	Lists statistical information related to missing security updates, found on scanned computers.
Computer Summary	A summary of scan target information, including: <ul style="list-style-type: none"> • Operating system information • Agent status • Vulnerabilities severity.
Hardware Audit	Illustrates information related to the hardware found during an audit.
Computer Details	Provides a detailed list of computer properties, including: <ul style="list-style-type: none"> • MAC Address • Time to Live • Network Role • Domain • Lan Manager • Is relay agent • Uses relay agent • Attributes • Operating system • IP address.
Open Shares	Lists all the shared folders found during an audit. The results are grouped by computer name.
Open Ports	Lists all the open ports found during an audit. The results are grouped by port type (TCP and UDP).
Services	Lists all services found during an audit. Results are grouped by computer name.
Groups and Users	Lists all Groups and Users found during an audit. The result is grouped by computer name.

Report Title	Description
Mobile Device Policies	Lists all mobile device policies found during an audit. The result is grouped by computer name.
Unauthorized Applications	Lists all unauthorized applications installed scan targets, including: <ul style="list-style-type: none"> • Top Computers with Unauthorized Applications • Top Unauthorized Applications • Applications Inventory • Computers without Antivirus Installed
Antivirus Applications	Shows information related to the antivirus installed on scan targets.
New Devices	Lists all new devices found during last week audits.

Legal Compliance reports

To view **Legal Compliance** reports:

1. Click **Reports** tab.
2. From the list of reports, expand any of the following compliance reports suites:

Report Suite Title	Description
PCI DSS Compliance Reports	<p>The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. GFI LanGuard provides you with a number of reports that cater for PCI DSS compliance, including:</p> <ul style="list-style-type: none"> • PCI DSS Requirement 1.4 - Installed Firewall Applications • PCI DSS Requirement 2.2.3 - Disk Encryption Applications • PCI DSS Requirement 5.2 - Antivirus Applications • PCI DSS Requirement 6.1 - Remediation History by Date • PCI DSS Requirement 12.12 - Open Trojan Ports by Host.
HIPAA Compliance Reports	<p>The Health Insurance Portability and Accountability Act (HIPAA) is a requirement of all healthcare providers that regulates the exchange of private patient data. This helps prevent unlawful disclosure or release of medical information. To help you follow HIPAA regulations, GFI LanGuard provides you with a suite of HIPAA compliance reports, including:</p> <ul style="list-style-type: none"> • HIPAA 164.308(a)(1)(ii)(A) - Missing Security Updates by Host • HIPAA 164.308(a)(1)(ii)(A) - Vulnerability Distribution by Host • HIPAA 164.308(a)(4)(ii)(A) - Open Ports • HIPAA 164.308(a)(5)(ii)(D) - Audit Policy • HIPAA 164.308(a)(8) - Baseline Changes Comparison.

Report Suite Title	Description
SOX Compliance Reports	<p>The Sarbanes-Oxley Act (SOX) is regulation created in response to high-profile financial scandals as well as to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. GFI LanGuard provides a list of SOX compliance reports, including:</p> <ul style="list-style-type: none"> • SOX 302.a - Network Vulnerability Summary • SOX 302.a - Remediation History by Host • SOX 302.a - Security Scans History • SOX 404 - Vulnerability Listing by Category • SOX 404 - Missing Security Updates by Host.
GLBA Compliance Reports	<p>The Gramm–Leach–Bliley Act (GLBA) is an act that allows consolidation between Banks and Insurance companies. Part of the act focuses on IT network compliance for such companies. GFI LanGuard offers a list of GLBA Compliance reports, including:</p> <ul style="list-style-type: none"> • GLBA 501.b - Baseline Changes Comparison • GLBA 501.b - Network Patching Status • GLBA 501.b - Open Trojan Ports by Host • GLBA 501.b - Vulnerable Hosts Based on Open Ports • GLBA 501.b - Vulnerable Hosts by Vulnerability Level.
PSN CoCo Compliance Reports	<p>The Public Service Network - Code of Connection (PSN CoCo) is simply a list of conditions that should be met before connecting an accredited network to another accredited network. GFI LanGuard helps you monitor the status of such connections through the list of PSN CoCo Compliance reports, which include:</p> <ul style="list-style-type: none"> • PSNCoCo RIS. 1 - Baseline Changes Comparison • PSNCoCo MAL. 1 - Disk Encryption Applications • PSNCoCo MAL. 1 - Installed Firewall Applications • PSNCoCo PAT. 1 - Installed Security Updates by Host • PSNCoCo PAT. 1 - Installed Security Updates by Severity.
CIPA	<p>The Children's Internet Protection Act (CIPA) addresses concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. GFI LanGuard Central Management Server provides a list of CIA Compliance reports including:</p> <ul style="list-style-type: none"> • Req. 47 USC § 254(l)(1)(A)(iv) - Network Vulnerability Summary • Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Distribution by Host • Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Category • Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Host • Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Severity

Report Suite Title	Description
	<ul style="list-style-type: none"> • Req. 47 USC § 254(l)(1)(A)(iv) - Open Trojan Ports by Host • Req. 47 USC § 254(l)(1)(A)(iv) - Network Patching Status • Req. 47 USC § 254(l)(1)(A)(iv) - Missing Security Updates by Host • Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts by Vulnerability Level • Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts Based on Open Ports • Req. 47 USC § 254(l)(1)(A)(iv) - Remediation History by Host • Req. 47 USC § 254(l)(1)(A)(iv) - Remediation History by Date • Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Host • Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Date • Req. 47 USC § 254(l)(1)(A)(iv) - Baseline Changes Comparison
FERPA Compliance Reports	<p>The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. GFI LanGuard provides a list of FERPA Compliance reports, including:</p> <ul style="list-style-type: none"> • FERPA 20 USC 1232g (b) - Network Patching Status • FERPA 20 USC 1232g (b) - Network Security Log by Host • FERPA 20 USC 1232g (b) - Remediation History by Date • FERPA 20 USC 1232g (b) - Vulnerability Distribution by Host • FERPA 20 USC 1232g (b) - Vulnerable Hosts Based on Open Ports.
ISO/IEC 27001 & 27002 Compliance Reports	<p>The Information technology – Security techniques – Information security management systems (ISO/IEC) standard formally specifies a management system that is intended to bring information security under explicit management control. GFI LanGuard offers an extensive list of ISO/IEC Compliance reports, including:</p> <ul style="list-style-type: none"> • ISO/IEC 27001 A. 10.4 - Antivirus Applications • ISO/IEC 27001 A. 10.7.2 - Disk Encryption Applications • ISO/IEC 27001 A. 10.6.2 - Open Shares • ISO/IEC 27001 A. 10.6.2 - Services • ISO/IEC 27001 A. 10.6.2 - System Information.
FISMA Compliance Reports	<p>The Federal Information Security Management Act (FISMA) assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. GFI LanGuard helps</p>

Report Suite Title	Description
	<p>you be compliant to FISMA standards through the provided reports, which include:</p> <ul style="list-style-type: none"> • FISMA NIST SP 800-53 AC-2 - Groups and Users • FISMA NIST SP 800-53 PM-5 - Computer Details • FISMA NIST SP 800-53 PM-5 - Computer Summary • FISMA NIST SP 800-53 SI-5 - Missing Security Updates by Host • FISMA NIST SP 800-53 SI-7 - Antivirus Applications.
CAG Compliance Reports	<p>The Consensus Audit Guidelines (CAG) is a publication of best practice guidelines for computer security. The project was initiated as a response to extreme data losses experienced by organizations in the US defense industrial base. GFI LanGuard offers a list of CAG Compliance reports, including:</p> <ul style="list-style-type: none"> • CAG CC1 - Hardware Audit • CAG CC1 - Scan History • CAG CC3 - Audit Policy • CAG CC3 - Low Security Vulnerabilities • CAG CC11 - Open Ports.
NERC CIP Compliance Reports	<p>The North American Electric Reliability Corporation (NERC) develops standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient. GFI LanGuard provides a list of NERC CIP Compliance reports, including:</p> <ul style="list-style-type: none"> • NERC CIP-005 R2 - Installed Firewall Applications • NERC CIP-005 R2 - Open Ports • NERC CIP-007 R2 - Open Shares • NERC CIP-007 R2 - Services • NERC CIP-007 R2 - System Information.

Security and compliance in SQL Server

The primary purpose of any database management system is to store and provide accurate information as requested by other software clients. Security of the database system and the information it keeps is another crucial component. There are many aspects of SQL Server security configuration, such as authentication, server and database roles, ownership, or Common Language Runtime (CLR) integration. However, in this article, we'll focus on those that are related to (and common for) most of compliance regulations.

Each compliance regulation (e.g. GDPR, PCI, HIPAA, GLBA, Basel II, FERPA, or SOX) requires a certain security level. After analyzing all of the compliance regulations, it is to be concluded that they have in common many requirements – primary about data security via database system and data access auditing.

Nikhil Yadav (nikhil27rock@gmail.com)

Being compliant doesn't also guarantee you're safe. If you audit more than the specific compliance regulations minimum is, it's OK as it provides higher safety. On the other hand, logging too much will make unnecessary overhead; we'll focus on necessary compliance auditing that's related to SQL Server security.

The following requirements are common for the compliance regulations in terms of security:

- Secure and up to date database system that hosts information
- Precisely defined access rules, with minimum needed permissions for appropriate and valid information access
- Auditing of logon attempts – both successful and failed
- Auditing of all actions and changes applied to roles, users, and databases

General recommendations for security and compliance in SQL Server

The following SQL Server security related actions are generally recommended to be taken for accomplishing the compliances.

- Set up a SQL Server environment that's secure and monitored constantly. Provide the SQL Server system with continuous event auditing, whether the events are internal or external, invoked by the system or users. Enforce strict rules that unauthorized parties cannot change and apply the rules to logins, databases, users, tables, and any SQL Server object.

In short, ensure the security and confidentiality of the data using proper user permissions and limitations.

However, regardless of the strict rules set, compliance regulations for SQL Server requires auditing and periodical analysis of all events related to security – including the events were performed by users or members of administrative personnel. Any permission changes on the SQL Server objects, and access to databases/tables with confidential records must be documented.

Each and every compliance regulation requires that users and members of administrative personnel are treated equally in the process of SQL Server auditing and providing audit information to auditors.

- Use secure and officially verified hardware and software for accessing SQL Server data. There are common potentially high security configuration omissions, such as default network settings, logins, and passwords often used by attackers.

Any supplied default SQL Server system security parameters should be modified. It's recommended not to use the mixed mode (enables both Windows and SQL Server authentication) for authentication. Instead, switch to the Windows authentication

only – that will enforce the Windows password policy – checking of the password length, life duration, and history. The feature of the Windows password policy that makes it different from the SQL Server authentication is the login lockout – after a number of successive failed logon attempts the login becomes locked and unusable for further use.

On the other hand, the SQL Server authentication does not provide any methods for detecting brute-force attack attempts, and what's worse, SQL Server is even optimized for handling large numbers of rapid login attempts. So, if the SQL Server authentication is a must in a particular SQL Server system, it's highly recommended to disable the SA login.

- Disable features and services in SQL Server that are not required for proper running of the database system. Many SQL Server components require additional set up and modification of their default settings. By omitting such components, additional potential security issues are avoided. Install only what you need.
- Periodically check and verify the SQL Server security configuration, along with rules and permissions previously defined. Any change that is not documented can be a potential security issue and lead to losing the database system compliance status.

SQL Server security and compliance auditing requirements

Compliance regulations specify only what the requirements are, not how to achieve them. The general requirement is to ensure the confidentiality, integrity, and proper availability of sensitive information, but the process is not explained. However, it's mandatory to audit, document and provide reports for all security related events on the SQL Server instance, database, and object levels in order to be compliant.

It's up to an auditor to request different types of SQL Server events audit reports related to security and providing adequate documentation is not an easy task.

ApexSQL Audit is a [SQL Server auditing tool](#) that can track and document all security related events, based on user selection, including password and login changes, logon attempts, and access to all or specific SQL Server objects. As an output, it provides a variety of built-in reports that can help in terms of compliance and in detecting potential SQL Server security issues.

ApexSQL Audit helps with being compliant and discovering security risks as it:

- Automatically monitors events to make sure compliance rules are met
- Provides accurate and relevant reports for compliance reviews
- Provides reports that discover risks and vulnerabilities
- Identifies compliance and security vulnerabilities

SQL Server security configuration changes

Changes applied to SQL Server settings related to security must be monitored and documented for the compliances purpose. On the other hand, this information can indicate potential security risks and omissions.

There are several reports in ApexSQL Audit that show captured events that modified the SQL Server security configuration:

- The report Security configuration history provides history of changes on SQL Server logins, roles, and users. It shows changes on password and username, a created or dropped entity, and entity permission changes:

Date	Server	Database	Login	Application	Client host	Schema	Object	Operation	Access list	State
02/05/2018 09:32:34.871 PM	DESKTOP-7E958TV									N/A
User "DESKTOP-7E958TV\dpepi" updated auditing filter for "DESKTOP-7E958TV" (simple): Login is "sa" AND (Operation is one of ("AlterCertificate", "AlterCredential", "AlterDatabase", "AlterEndpoint", "AlterLogin", "AlterServerRole", "AlterServerTrigger", "CreateCredential", "CreateDatabase", "CreateEndpoint", "CreateEventNotification", "CreateLogin", "CreateServerRole", "CreateServerTrigger", "DropCredential", "DropDatabase", "DropEndpoint", "DropEventNotification", "DropLogin", "DropServerRole", "DropServerTrigger"))										

- The Permission changes report shows permission changes for a particular security entity that is monitored:

Date	Server	Database	Login	Application	Client host
01/11/2018 02:32:54.763 AM	DESKTOP-7E958TV	master	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio	DESKTOP-7E958TV
GRANT ALTER ANY EVENT NOTIFICATION TO [CLUSTER\DCadmin]					
01/11/2018 02:32:54.763 AM	DESKTOP-7E958TV	master	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio	DESKTOP-7E958TV
GRANT ALTER ANY ENDPOINT TO [CLUSTER\DCadmin]					
01/11/2018 02:32:54.763 AM	DESKTOP-7E958TV	master	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio	DESKTOP-7E958TV
GRANT ALTER ANY DATABASE TO [CLUSTER\DCadmin]					
01/11/2018 02:32:54.763 AM	DESKTOP-7E958TV	master	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio	DESKTOP-7E958TV
GRANT ALTER ANY CREDENTIAL TO [CLUSTER\DCadmin]					
01/11/2018 02:32:54.760 AM	DESKTOP-7E958TV	master	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio	DESKTOP-7E958TV
GRANT ALTER ANY CONNECTION TO [CLUSTER\DCadmin]					
01/11/2018 02:32:54.760 AM	DESKTOP-7E958TV	master	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio	DESKTOP-7E958TV
GRANT ALTER ANY AVAILABILITY GROUP TO [CLUSTER\DCadmin]					

SQL server security and data access

Monitoring user access to data is a must to meet compliance requirements. Each access must be tracked, being illegitimate or not. Also, as compliance regulations require without exceptions, actions performed by administrative personnel must be audited too

The information about the data access is provided with the following ApexSQL Audit audit reports:

Nikhil Yadav (nikhil27rock@gmail.com)

- The Access history report provides a history of user access to SQL Server databases and tables. Moreover, exact procedures and T-SQL statements used to access monitored objects are documented for each access attempt. Any access to a SQL Server object by a user not supposed to have such permission is an alert to check and verify permission parameters for the particular user and accessed object

Date	Server	Database	Login	Application
01/11/2018 01:09:49.110 AM	DESKTOP-7E958TV	AdventureWorks2014	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio
<pre> SELECT CAST(tbl.is_remote_data_archive_enabled AS bit) AS [RemoteDataArchiveEnabled], CAST(ISNULL(rdat.migration_state, 0) AS tinyint) AS [RemoteDataArchiveDataMigrationState] FROM sys.tables AS tbl LEFT OUTER JOIN #tmp_extended_remote_data_archive_tables AS rdat ON rdat.object_id = tbl.object_id WHERE </pre>				
01/11/2018 01:09:47.570 AM	DESKTOP-7E958TV	AdventureWorks2014	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio - Query
<pre> SELECT [Name], [ProductNumber] FROM [Production].[Product] WHERE [SafetyStockLevel]<@1 </pre>				
01/11/2018 12:31:10.883 AM	DESKTOP-7E958TV	AdventureWorks2014	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio - Query
<pre> SELECT [Name], [ProductNumber] FROM [Production].[Product] WHERE [SafetyStockLevel]<@1 </pre>				
01/11/2018 12:28:47.563 AM	DESKTOP-7E958TV	AdventureWorks2014	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio - Query
<pre> SELECT [Name], [ProductNumber] FROM [Production].[Product] WHERE [SafetyStockLevel]<@1 </pre>				
01/11/2018 12:27:47.610 AM	DESKTOP-7E958TV	AdventureWorks2014	MicrosoftAccount\d.pepic@hotmail.com	Microsoft SQL Server Management Studio - Query
<pre> SELECT TOP (1000) [ProductID] , [Name] , [ProductNumber] , [MakeFlag] , [FinishedGoodsFlag] </pre>				

Logons to the SQL Server database system

Each of the compliance regulations requires user logons to the system to be tracked and documented –every logon event must be captured, unsuccessful or not. Again, with no exceptions, logon attempts by administrative personnel must be audited.

Audited information about logon events are provided with the following ApexSQL Audit reports:

- The Logon activity history report provides all logon attempts, both successful and unsuccessful. Each logon attempt is listed with the SQL Server instance, application, application host name, logon status, time, and used login name.
- The Unauthorized access report is similar to the previous report, but narrowed to the failed logon attempts. It can indicate attacks and provide information on attack targets – specific login names and SQL Server instances. Report entries represent failed logons, caused by use of non-existing login names or wrong passwords:

Date	Server	Database	Login	Application	Client host	Schema
02/07/2018 10:42:57.280 AM	DESKTOP-7E958TV	master	sa	Microsoft SQL Server Management Studio	DESKTOP-7E958TV	
Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: <local machine>]						
02/07/2018 10:42:55.200 AM	DESKTOP-7E958TV	master	sa	Microsoft SQL Server Management Studio	DESKTOP-7E958TV	
Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: <local machine>]						
02/07/2018 10:42:48.267 AM	DESKTOP-7E958TV	master	sa	Microsoft SQL Server Management Studio	DESKTOP-7E958TV	
Login failed for user 'sa'. Reason: Password did not match that for the login provided. [CLIENT: <local machine>]						
02/07/2018 10:42:00.790 AM	DESKTOP-7E958TV	master		Microsoft SQL Server Management Studio	DESKTOP-7E958TV	
Login failed for user ''. Reason: An attempt to login using SQL authentication failed.						

As described, brute-force attacks are hard to indicate when the mixed authentication mode is used for the SQL Server database system authentication. The Unauthorized access report can easily indicate such attacks with numerous failed logons using the same username.

Complying with the regulations requires certain SQL Server security level, verified by appropriate auditing reports. The auditing reports ensure the compliance requirements, and help in identifying compliance and SQL Server security vulnerabilities. ApexSQL Audit with a range of auditing configuration options and a variety of comprehensive reports, makes [SQL Server auditing](#) easy, while ensuring security and compliance in SQL Server.

SQL Server database security auditing

The following auditing implementations are recommended on a database level as part of any database security auditing system:

1. Schema level auditing:
 - DDL activity
 - Changes made to stored procedures and triggers
 - Changes to privileges, users, and security attributes
2. Data level auditing:
 - Changes to sensitive data (DML activity)
 - SELECT statements
3. Any changes of the auditing settings

There are some native database security auditing solutions that can help fulfilling these requirements.

Schema level auditing

DDL commands are from the security standpoint have a high potential for malicious use and can be easily used to compromise any database system.

There are few ways to audit DDL activity:

Nikhil Yadav (nikhil27rock@gmail.com)

- SQL Server Audit feature or SQL Server trace files
- DDL triggers
- Schema snapshot comparison

For the purpose of this article, we will not consider DDL triggers and schema snapshot comparison in favor of SQL Server Audit and trace files.

The SQL Server Audit feature is native SQL Server auditing based on SQL Server extended events. Introduced with SQL Server 2008, it is the least intrusive auditing method and thus generally recommended for DDL activity auditing. It can store the audit events whenever they occur into the security log or the application event log, but the recommended method, which will be described in this article, is storing of audited events in the audit file.

Note: The database level activity auditing, and thus database security auditing using SQL Audit is reserved for SQL Server Enterprise and SQL Server Developer editions only.

To establish database security auditing using SQL Audit, the first step is creating the SQL Audit object. This can be done using T-SQL or via SQL Server Management Studio.

To create an SQL Audit object that will be used for database security auditing, the following T-SQL creation script can be used.

```
USE [master]

GO

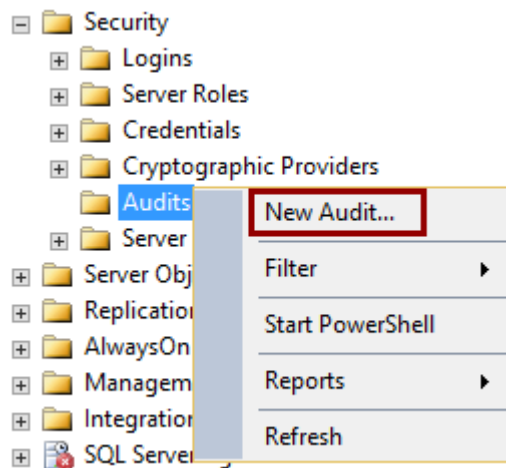
CREATE SERVER AUDIT [Audit ADW2014 DDL ]
TO FILE
(
    FILEPATH = N'C:\SQLAudits\'
    ,MAXSIZE = 20 MB
    ,MAX_FILES = 20
    ,RESERVE_DISK_SPACE = ON
)
WITH
(
    QUEUE_DELAY = 1000
    ,ON_FAILURE = CONTINUE
    ,AUDIT_GUID = '928b1094-b02b-437d-a5c7-8266af853b57'
)

ALTER SERVER AUDIT [Audit ADW2014 DDL ] WITH (STATE = ON)
```

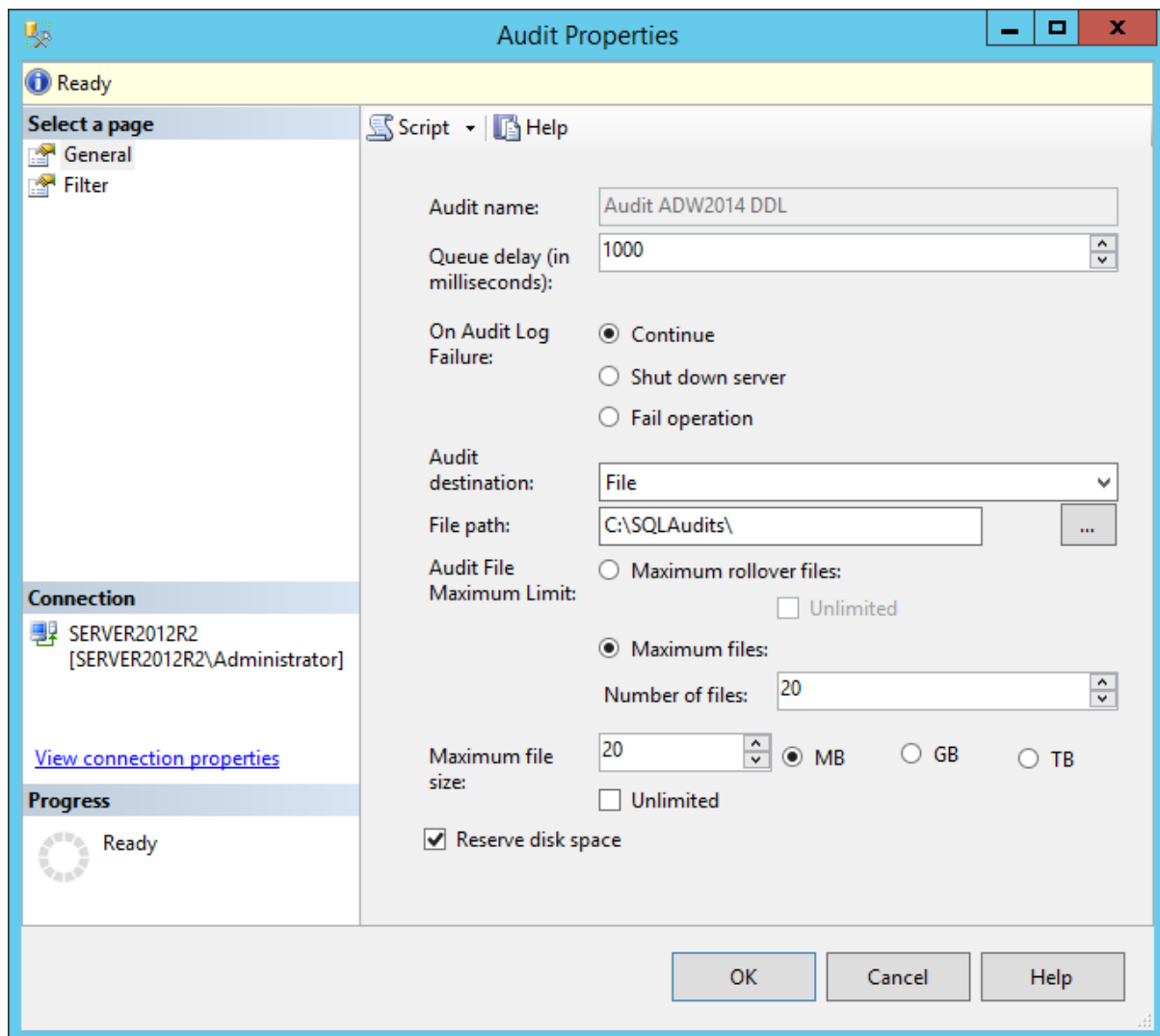
Nikhil Yadav (nikhil27rock@gmail.com)

GO

To use SQL Server Management Studio, locate the Security->Audits folder in the Object Explorer and chose the New Audit from the context menu.



In the Create Audit dialog that will be opened, select the Audit destination->File from the drop-down menu and determine the File path that will be used for storing the file where the audits will be logged.



All options in this dialog are self-explanatory and don't require additional explanations, but for those who are interested, more details can be found [here](#).

Once the SQL Server Audit object is created, the Database Audit Specifications object for the created audit object has to be set.

To create the Database Audit Specifications object for the above-mentioned auditing requirements, the following T-SQL could be used.

```
USE [AdventureWorks2014]
```

```
GO
```

```
CREATE DATABASE AUDIT SPECIFICATION [ADW2014 Auditing]
```

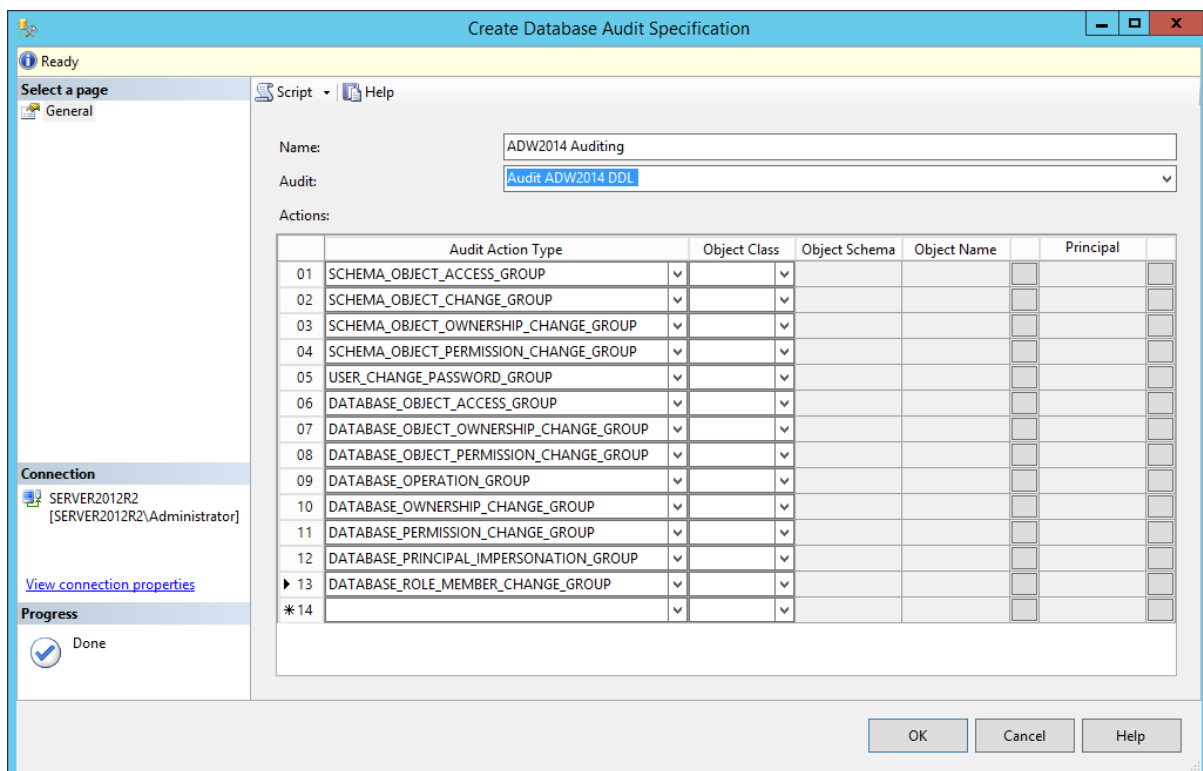
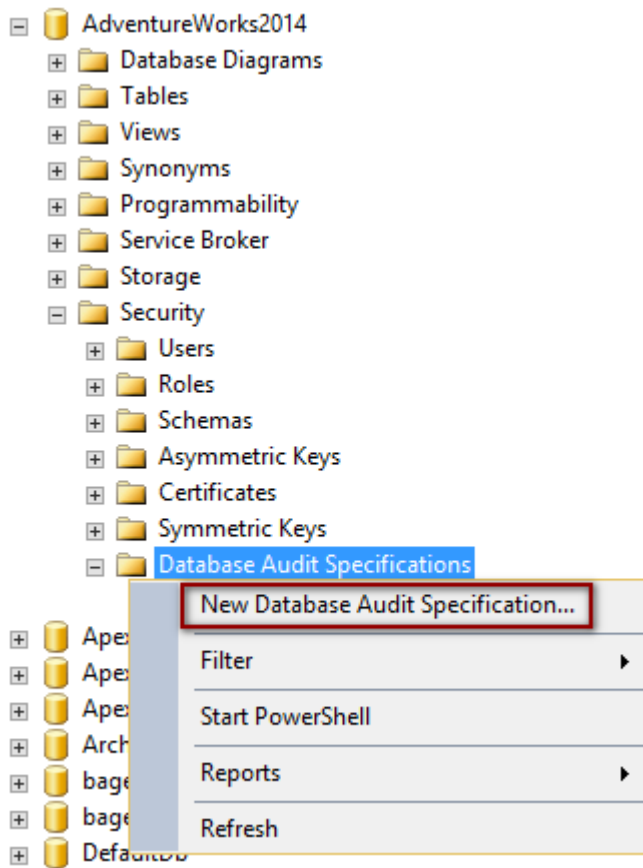
```
FOR SERVER AUDIT [Audit ADW2014 DDL]
```

Nikhil Yadav (nikhil27rock@gmail.com)

```
ADD (SCHEMA_OBJECT_ACCESS_GROUP),
ADD (SCHEMA_OBJECT_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (SCHEMA_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (USER_CHANGE_PASSWORD_GROUP),
ADD (DATABASE_OBJECT_ACCESS_GROUP),
ADD (DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP),
ADD (DATABASE_OBJECT_PERMISSION_CHANGE_GROUP),
ADD (DATABASE_OPERATION_GROUP),
ADD (DATABASE_OWNERSHIP_CHANGE_GROUP),
ADD (DATABASE_PERMISSION_CHANGE_GROUP),
ADD (DATABASE_PRINCIPAL_IMPERSONATION_GROUP),
ADD (DATABASE_ROLE_MEMBER_CHANGE_GROUP)

GO
```

The same could be done via SQL Server Management Studio's Object Explorer. Expand the database object tree, right click on the Security->Database Audit Specifications and select the New Database Audit Specification.



More details about the Create Database Audit Specifications object is available [here](#). Follow the links for additional details about [Database-Level Audit Action Groups](#).

Nikhil Yadav (nikhil27rock@gmail.com)

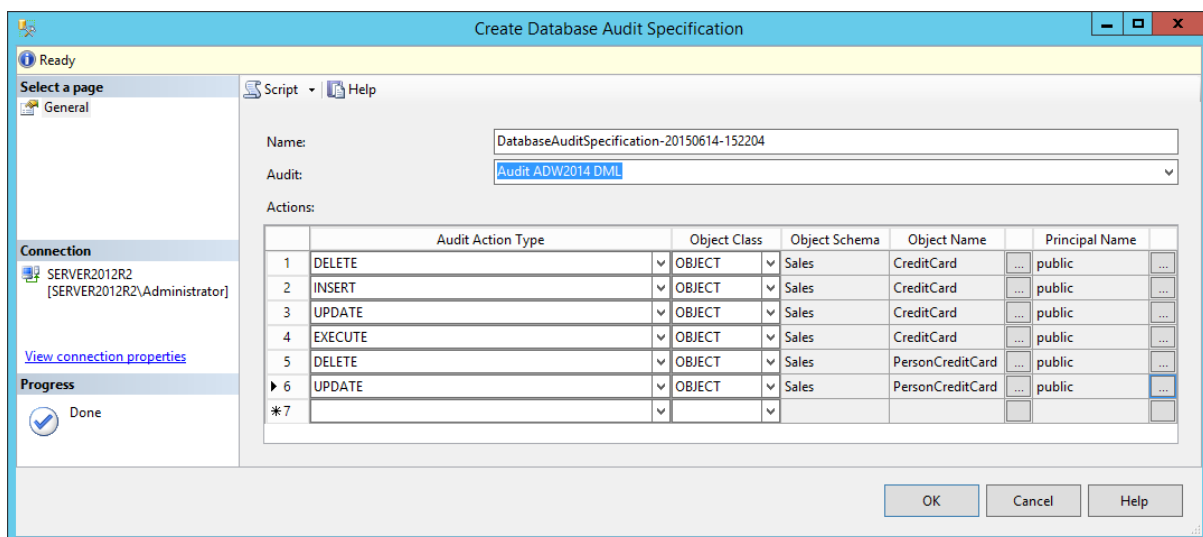
Note: The DATABASE_OBJECT_CHANGE_GROUP audits only the ALTER permission check on the SCHEMA as part of the CREATE statement. To actually audit CREATE, ALTER, or DROP operations on schema, the SCHEMA_OBJECT_CHANGE_GROUP must be added to the audit specification.

Once all the requirements for auditing were set, SQL Audit will start to collect and log every database structure change defined in the auditing specifications.

Data level auditing

Creating the SQL Audit and Database Audit Specifications objects for data is the same as the above and the only difference consists in setting different Database Audit Specifications.

After creating the new SQL Audit object for DML level auditing, that will be named Audit ADW2014 DML for the purpose of this article, it should be associated with the new Database Audit Specification object. For the purpose of the DML auditing, Database-Level Audit Actions SELECT, INSERT, UPDATE, DELETE and if needed EXECUTE operations have to be set for auditing. For more information visit [Database-Level Audit Actions](#).



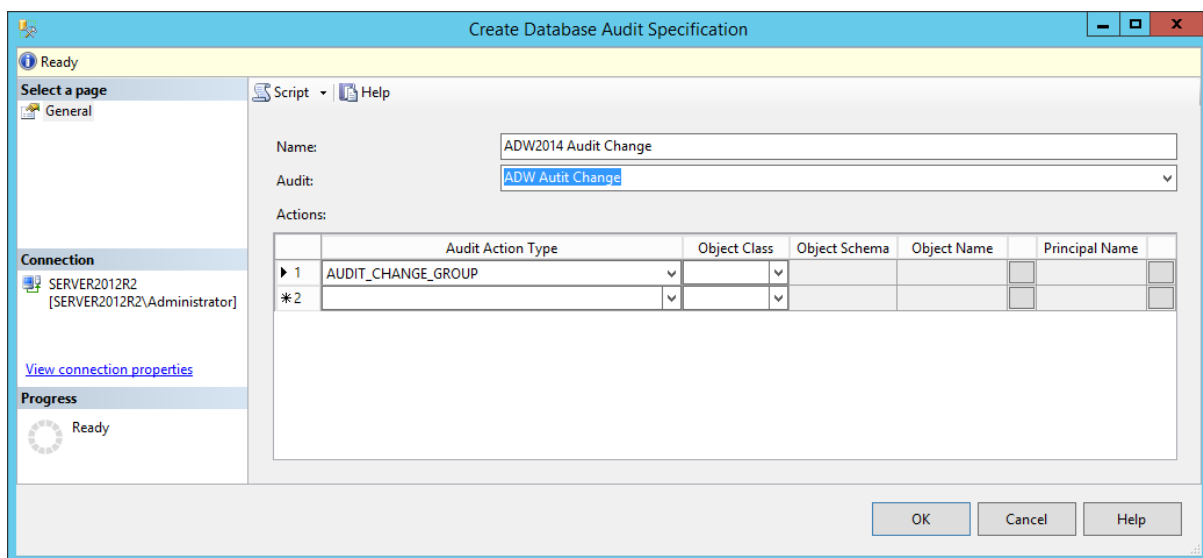
Since it is possible to specify just one object/principal per audit event, creating all the necessary audit specifications can be quite strenuous and cumbersome. This is especially evident when creating specifications for databases with even a bit larger amount of tables and views and when more principals have to be included in auditing. The above image is just an example where only a few specifications are defined.

Note: The audit type can be configured on Schema and Database object class, which means that all objects that belongs to the specified schema will be audited, as well as all objects within the selected database, if the database is specified as object class. This should be used carefully as torrent of unnecessary data may be collected and stored in the .audit files.

Nikhil Yadav (nikhil27rock@gmail.com)

Audit the audit

The easiest way for attacker to stay unnoticed is to temporarily change the definition of auditing settings or to change the collected data itself. In order to allow tracking of changes to audit and audits specifications objects, or better say to "audit the audit", SQL Server Audit Action Group AUDIT_CHANGE_GROUP is introduced starting with the SQL Server 2012. Besides tracking changes to audit and audits specifications objects, this group also track failed auditing and changes made to audit sessions. Once set on the Database Audit Specifications level, it will audit all changes made to database audit specifications within that database.



The AUDIT_CHANGE_GROUP audit action type will log an auditing event when any of the following commands are executed.

- Create server audit
- Create server audit specification
- Create database audit specification
- Alter server audit specification
- Alter database audit specification
- Alter server audit
- Drop server audit
- Drop server audit specification
- Drop database audit specification

ApexSQL Audit

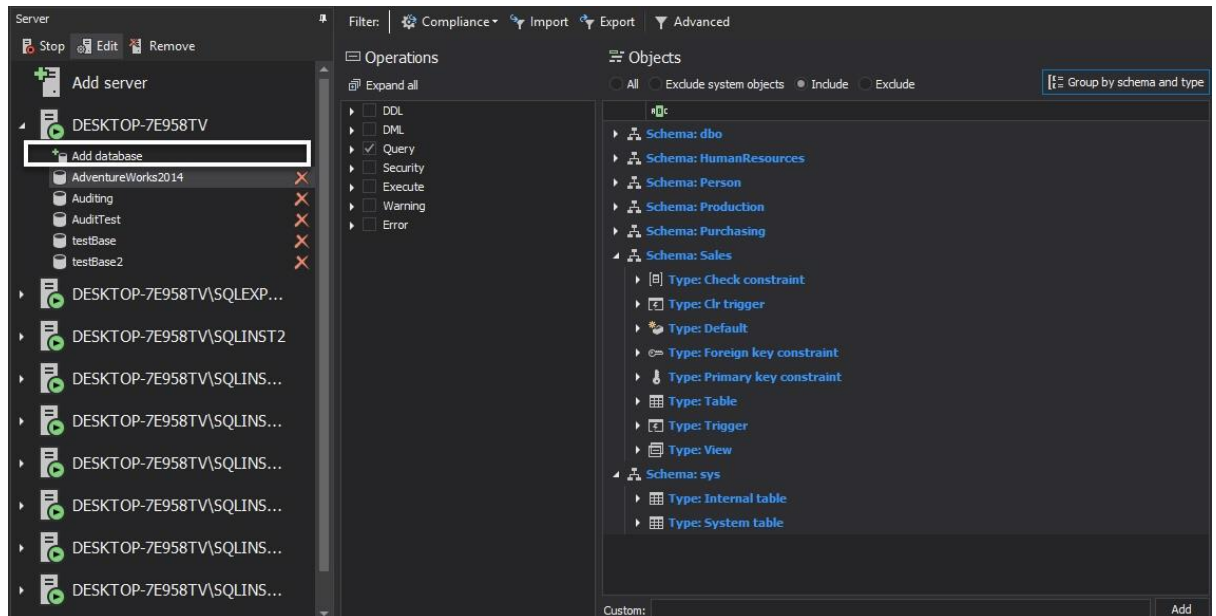
ApexSQL Audit is a [SQL Server auditing and compliance tool](#) capable to audit over 200 SQL events on SQL server and database level and to store them into a single tamper-evident central repository database. Collected information are easily available on request through eleven built-in reports with additional custom report that is designed around the advanced filtering which allows meeting even the most demanding user requirements.

NIKIL YADAV (nikhil2/rock@gmail.com)

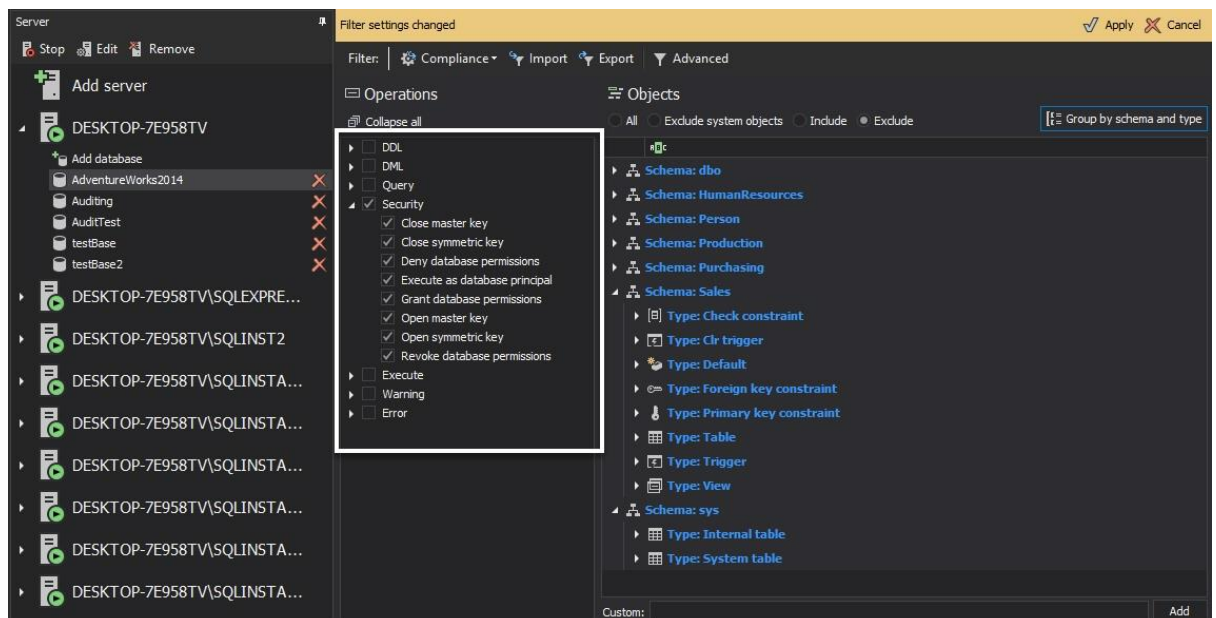
With ApexSQL Audit, database security auditing of schema and data activity can be set in a single pass while all changes on the auditing settings will be tracked by default.

To do that in the ApexSQL Audit GUI using the simple filter:

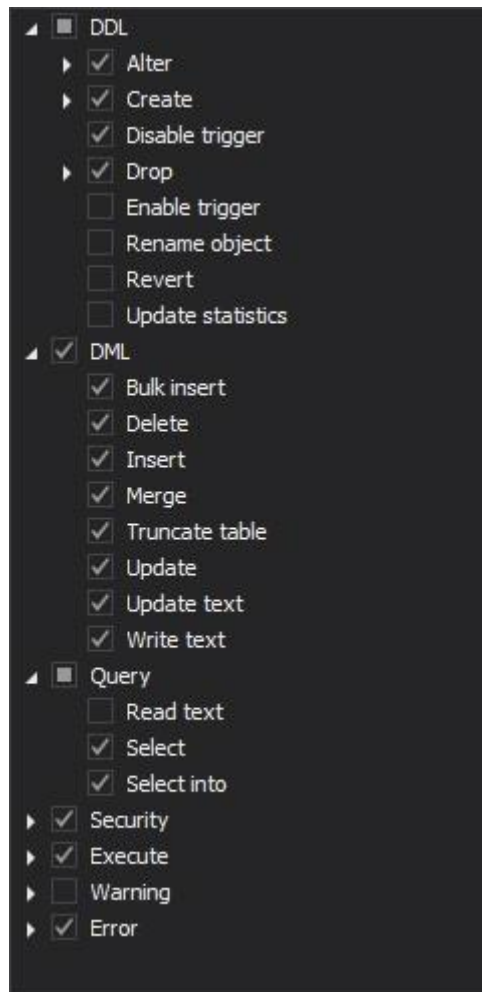
1. Select the database(s) to be audited using Add database



2. Set the required auditing filter conditions for each database added for auditing



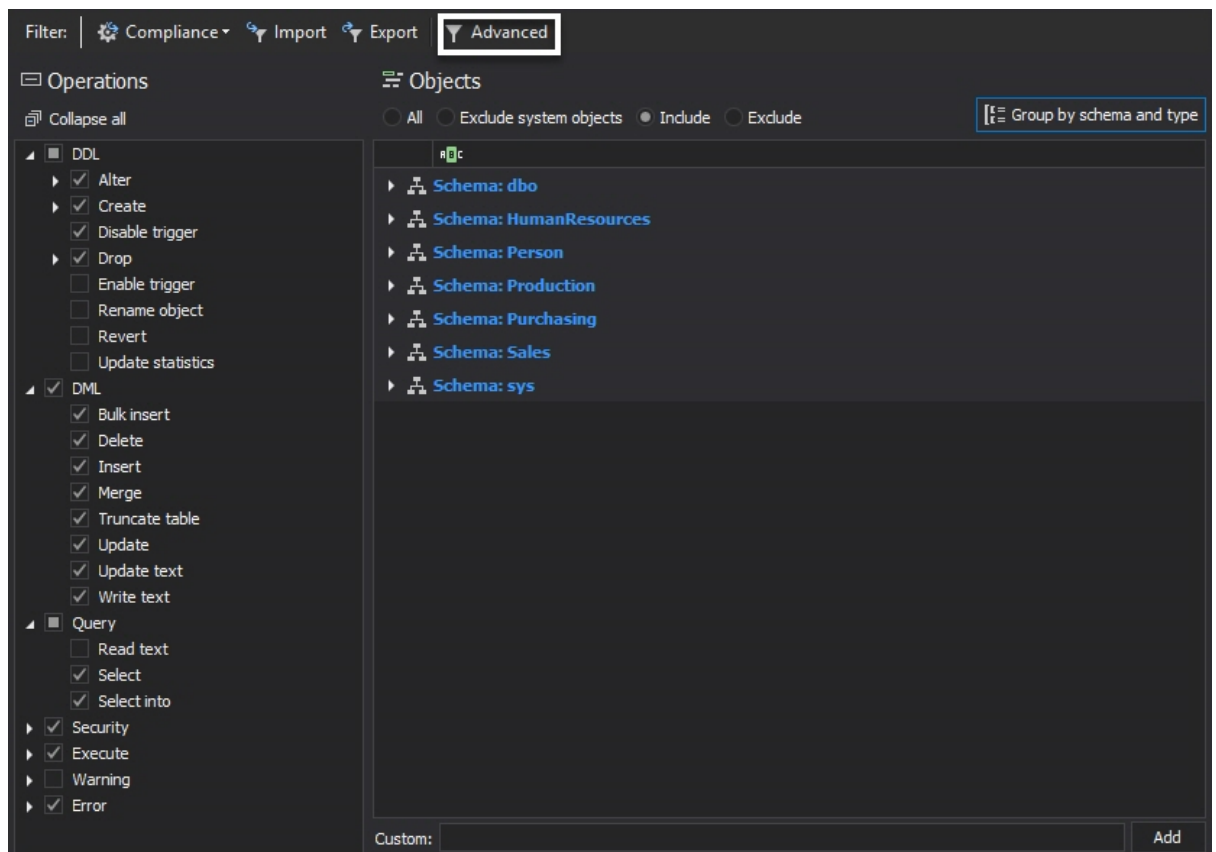
Below is the list of all available database level auditing filter selections with an example configuration



3. Press Apply in the pop-up bar at the top of the tab and this is it... this is all that has to be done to set up the database security auditing

Alternatively, to set up the auditing via the advanced filter:

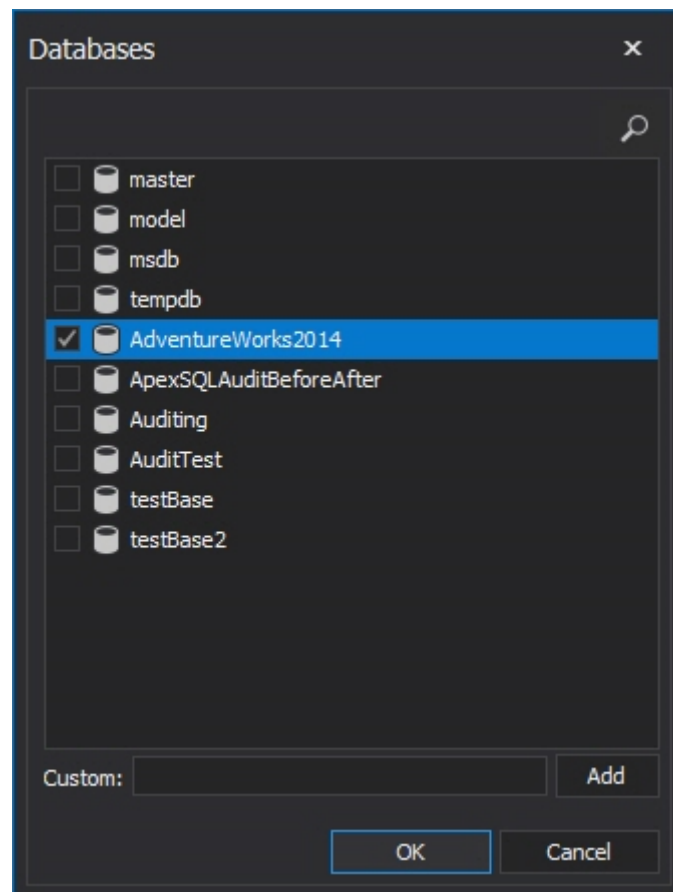
1. Check the Advanced radio button in the Filter type section

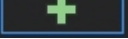


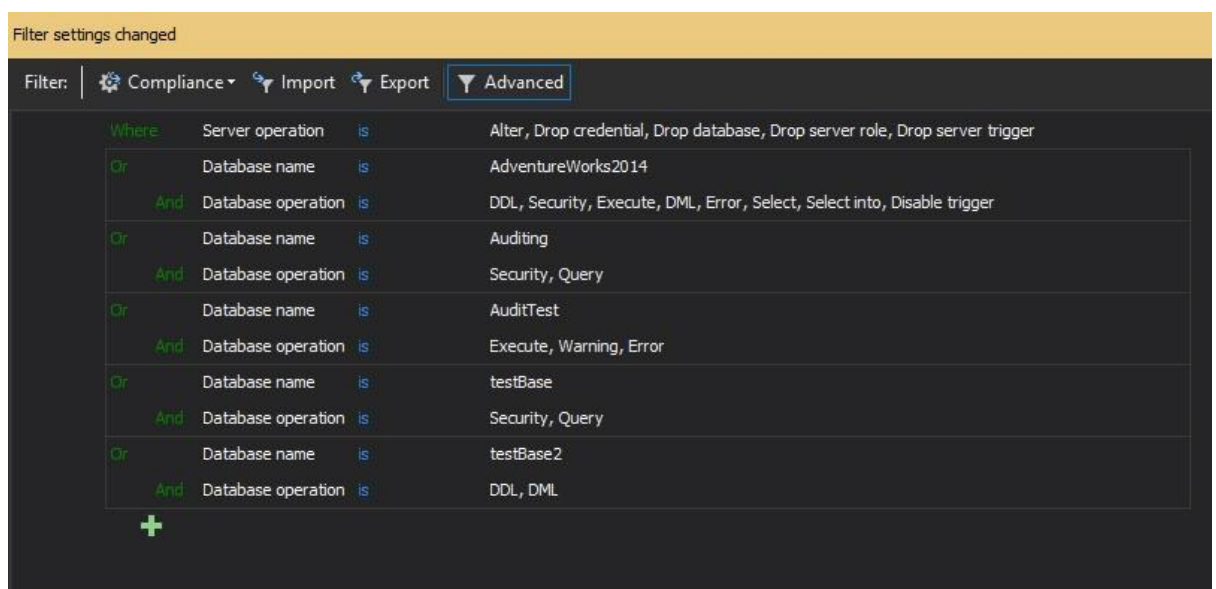
2. Press  to add the condition
3. Select the Database name data field



4. Click on <empty>



5. Press  again, select the Database operations data field and select the required operations, e.g. DDL, DML auditing etc.



6. Press Apply in the pop-up bar at the top of the tab



ApexSQL will now start to collect the audited events and to store the audited data into the central repository database

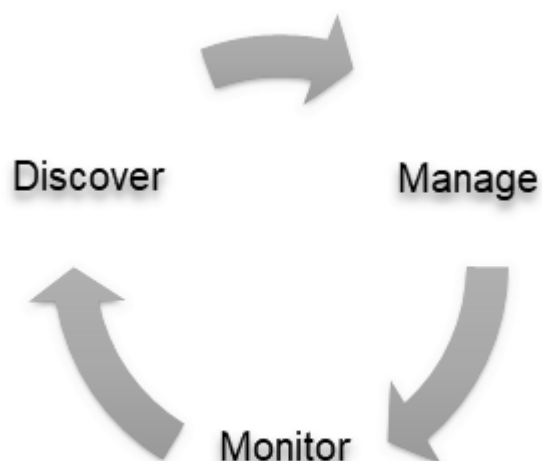
The requirements to track changes of the auditing settings is implemented by default in ApexSQL Audit and tracking the auditing settings cannot be disabled by user, making the auditing filters tamper evident. Every change in auditing setting along with precise information about the filter settings and who performed the change can be seen in the Audit settings history report

Database auditing – control and monitor sensitive data access in SQL Server

In the current cyberage, data protection and database auditing have been the number one priority for any organization. Control assessment procedures and techniques nowadays are heavily dependent on the compliance regulatory frameworks and their respective requirements.

This article is meant to dig deeper into this challenge and help with preparing proper techniques and control measures while monitoring access the activity in SQL Server databases via this 3 step notation:

- **Discover** – find where sensitive data resides in MS SQL databases
- **Manage** – employ control access measures
- **Monitor** – track database activity and monitor data access



Discover

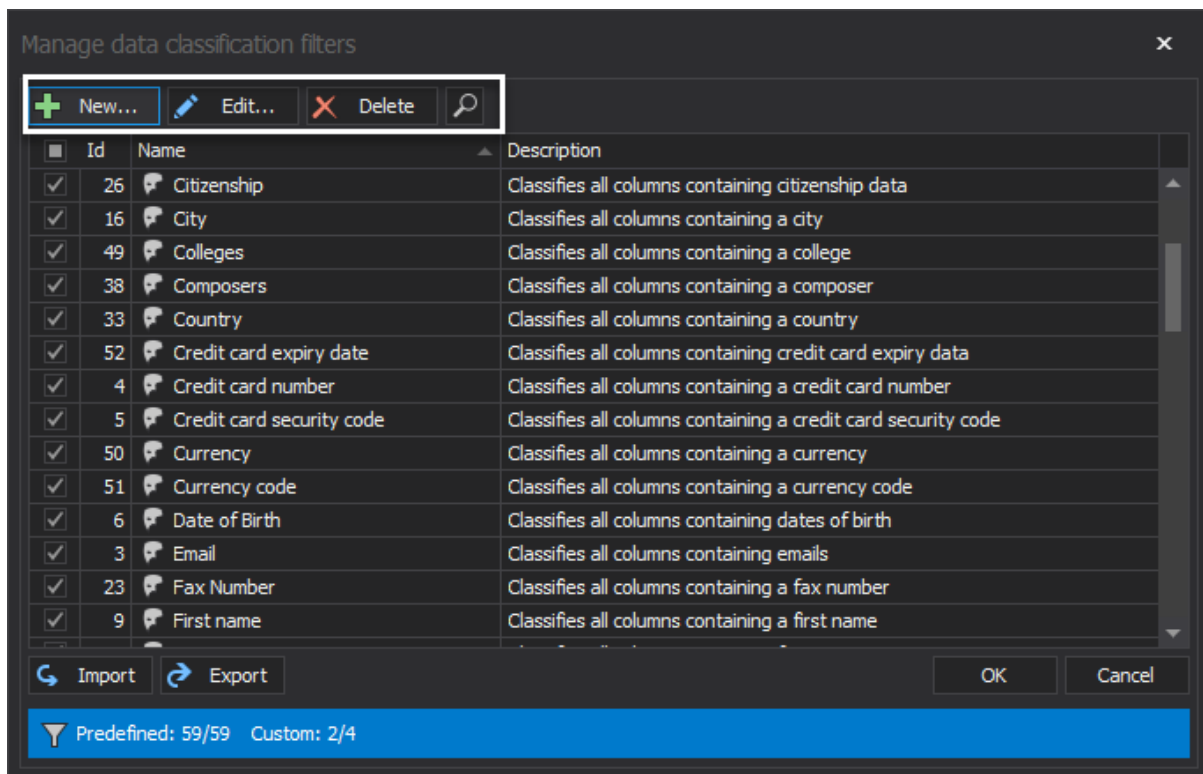
The discovery process is arguably the most important step to achieve aspired results. Sensitive data as a term might be relative depending on the information type or data origin, but no matter the cause, any information can be considered as sensitive as long as the data holder wouldn't like to share it.

With that said, compliance frameworks strive to describe and selectively explain what information type is considered as sensitive. Therefore, for many, sensitive data refers to personally identifiable information, but it can also refer to any business data when mishandled can hazard the privacy, economic, or social status of an individual or company.

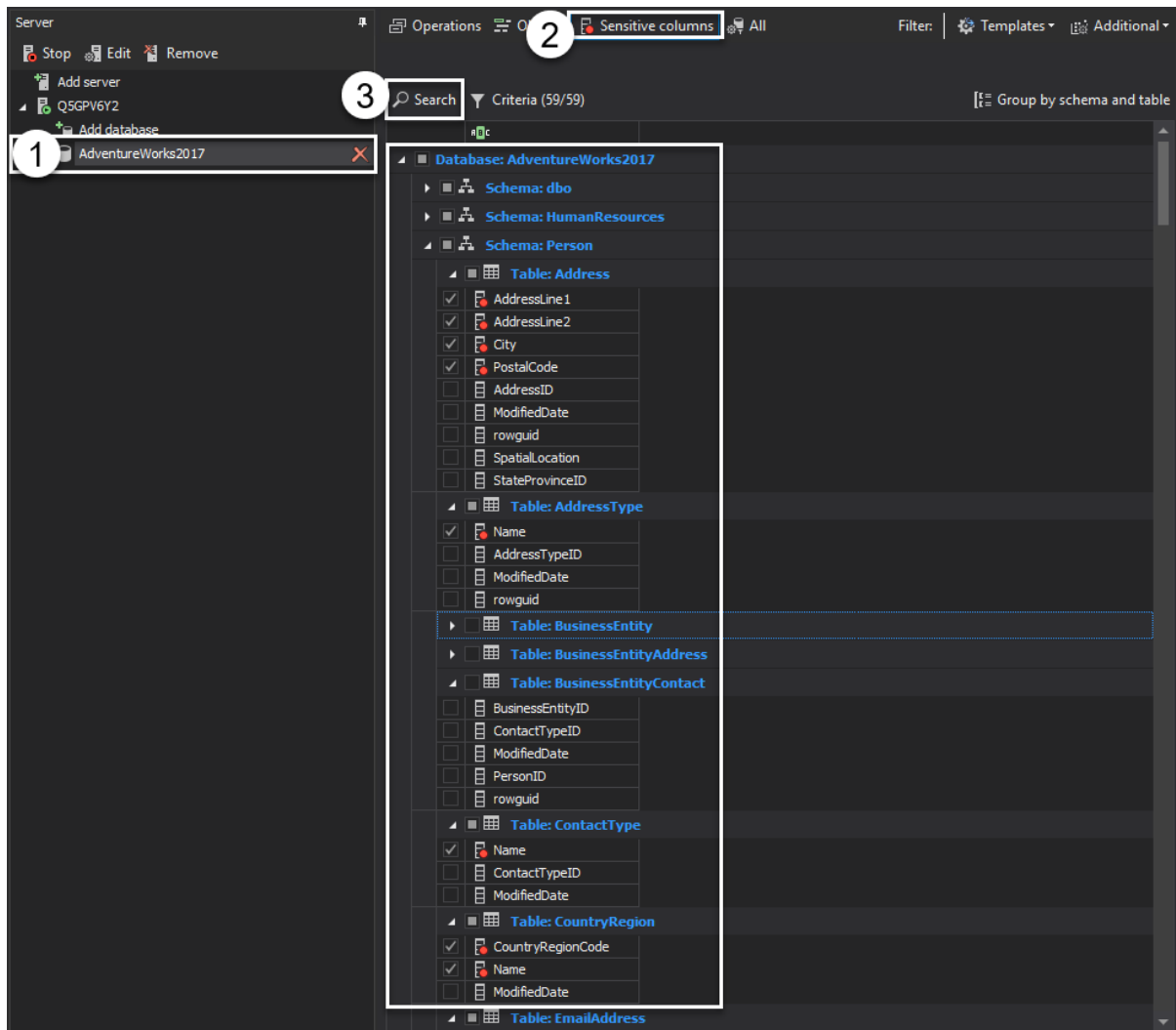
In this database auditing guide, we are about to explain how to find sensitive data in the MS SQL database. An efficient search means to pin down data attributes that make it sensitive first. Microsoft SQL allows the employment of native mechanisms to perform a search on databases, starting with the most primitive by querying metadata on "sys.columns" to find matching results on the column names, but also the empowered [Full-Text Search](#) to perform a rule-based search on data-level. Full-Text Search, as a mechanism, allows more in-depth search analysis and helps to identify information by combining multiple rules at once, which makes it a strong candidate to perform this step.

With constant data movement and procedures updates in complex IT infrastructures, native solutions can help identify sensitive data to a certain degree, but it is also time-consuming and error-prone process. [ApexSQL Audit](#) is a database auditing tool that provides the capability to search for sensitive data easily under multiple rules at once for any database in the SQL Server environment.

One can choose from 50+ pre-defined criteria rules to easily identify sensitive data but can also expand the search criteria via creating completely new or adjusting the pre-defined templates:



Once the specific attributes are pinned and included in the search criteria, the database exploration begins. As a pre-configuration step to track sensitive data access in ApexSQL Audit, searching for sensitive data based on a defined rule set is employed via a quick and easy action set, likewise demonstrated below:



Now, when we know where sensitive data resides in the SQL Server environment, questions like "What tables store sensitive information? How do we control sensitive data access?" can be easily addressed. With this database auditing solution, revealing exploiting points in data access leads to easier access control management.

Manage

Control data access

Protecting sensitive information, and control who can access the data is a high priority. Once the access points are understood, defining how the data is accessed and how to control unauthorized access are control measures to consider next.

So, the principle of least privilege, a method to assign the least required permissions for SQL Server principles accessing sensitive information, is a practice to follow. The next two paragraphs are meant to shed more light on how to achieve it, followed by employing a database auditing mechanism to track activity and recognize any anomaly behavior.

Nikhil Yadav (nikhil27rock@gmail.com)

Role-based authorization

It is important to make a plan that will provide both: access management and simplicity in defining authorization policies. With the [role-based](#) permission defining the approach, security policies are granted against specific roles, and therefore separation of duties is achieved while assuring granting policies are easily managed. Simple as it is, a certain user or group of users can be associated with a specific role, which is a map of security policies that picture the data access possibilities for associated users against the database.

Row-level security

After the database level policies are in place, row-level security is the next step in following the stellar security strategy. [Row-level security](#) allows one to enhance and polish the separation of duties model to a row-level degree. In simple words, it is a customized set of rules to define data access on the row level.

Let's assume we have two different users associated with the financial database. Bank employees can access data by divisions, Employee_1 is associated with the EMEA region, while Employee_2 is associated with the AMER region, both of them can interpret query to view data in the same manner, but the results are different for each. Here is an example overview to help to understand the RLS works:

Complete data records			Employee_1 records			Employee_2 records		
User	Division	Sales	User	Division	Sales	User	Division	Sales
Employee_1	EMEA	109000	Employee_1	EMEA	109000	Employee_2	AMER	205444
Employee_1	EMEA	106540	Employee_1	EMEA	106540	Employee_2	AMER	195375
Employee_2	AMER	205444	Employee_1	EMEA	119245	Employee_2	AMER	215432
Employee_2	AMER	195375						
Employee_1	EMEA	119245						
Employee_2	AMER	215432						

Controlling unauthorized access

Failed login attempts are commonly preceding unauthorized access, consider the fact that regularly mistyped credential information can trigger a faulting login attempt, we recommend to employ a database auditing mechanism so we can inspect what we expect.

Auditing failed login attempts

Regardless of the failed login attempt reasons, ApexSQL Audit provides a pre-defined reporting template to use and reconstruct complete information on failed logins against the audited SQL instance:

Date	Server	Database	Login	Application	Client host	Schema	Object	Operation	Access list	State
03-22-2018 04:25:11.537 PM	ZWERKA\SQL2014	master	Nesha	Microsoft SQL Server Management Studio	ZWERKA			Audit login failed		Failure
Login failed for user 'Nesha'. Reason: Could not find a login matching the name provided. [CLIENT: <local machine>]										
03-22-2018 04:18:19.220 PM	ZWERKA\SQL2014	master	TestAuditBA	Microsoft SQL Server Management Studio	ZWERKA			Audit login failed		Failure
Login failed for user 'TestAuditBA'. Reason: Could not find a login matching the name provided. [CLIENT: <local machine>]										
03-21-2018 03:56:51.883 PM	ZWERKA\SQL2014	master	ZWERKA\Nebojsa	ApexSQL Audit	ZWERKA			Audit login failed		Failure
Login failed for user 'ZWERKA\Nebojsa'. Reason: Failed to open the explicitly specified database 'ApexSQLAuditBeforeAfter'. [CLIENT: <local machine>]										

Taking into the consideration that activities with malicious intentions against sensitive information in a database bring high-risk consequences, it is highly recommended to employ an alerting mechanism to raise awareness whenever an unexpected event has occurred in a database. Therefore, ApexSQL Audit provides that capability with a comprehensive and [real-time alerting via e-mail notifications](#) whenever a specific event occurs.

In the example below, we configured alert rule to bring attention if any login other than "ApexSQLAuditDemo and sa" perform any database operation against "ApexSQLAuditDemo" database, or whenever a failed login attempt is recorded against the SQL Server:

Alert wizard

Unauthorized activity alert

Where Database name is ApexSQLAuditDemo
And Login name is not ApexSQLAuditDemo, sa
And Database operation is DDL, Security, Execute, DML, Query
Or Server operation is Audit login failed

☐ Case sensitive

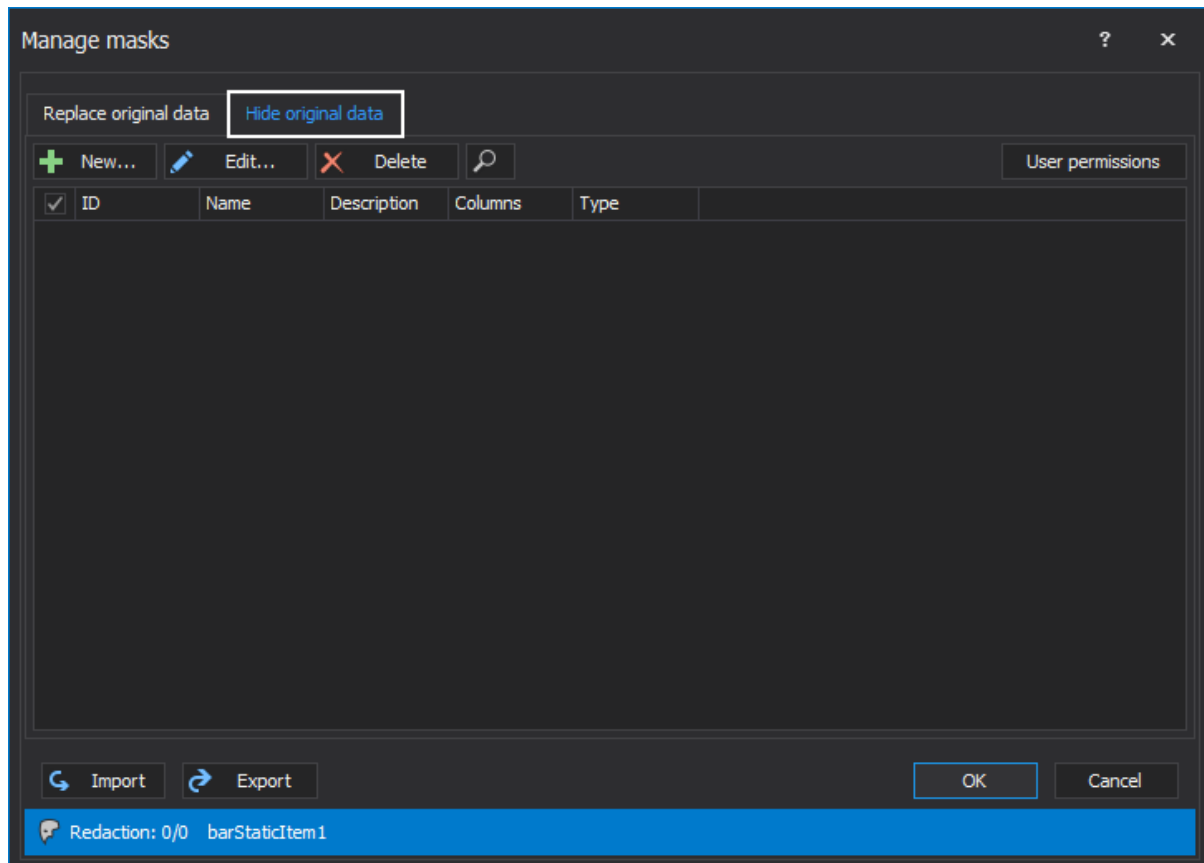
< Back Next > Cancel

Dynamic data masking

Dynamic data masking, as a feature, is available in Microsoft SQL Server 2016 and higher versions. The main purpose of this feature is to limit sensitive data exposure to unauthorized and non-privileged users, and therefore protect sensitive original information while serving the fake data instead.

Nikhil Yadav (nikhil27rock@gmail.com)

It is complementary to database auditing, and row-level security, which means this feature is meant to be used while combining all three of them to achieve a higher level of data protection and data access controls. With [ApexSQL Mask](#), which is a masking and data classification tool, dynamic data masking can be easily managed and define to whom original data will be exposed via easy to use and learn user interface:



To learn more about dynamic data masking in ApexSQL Mask, please consult [How to mask SQL Server data using Dynamic data masking](#) article.

Monitor – employ database auditing

Once the sensitive data is discovered, the control measures applied to follow the principle of least privileges and control data access, employing an auditing solution comes as the icing on the cake. Audit trail helps to inspect and understand database activity to prove if control measures are set up correctly or if there is still an area to improve it.

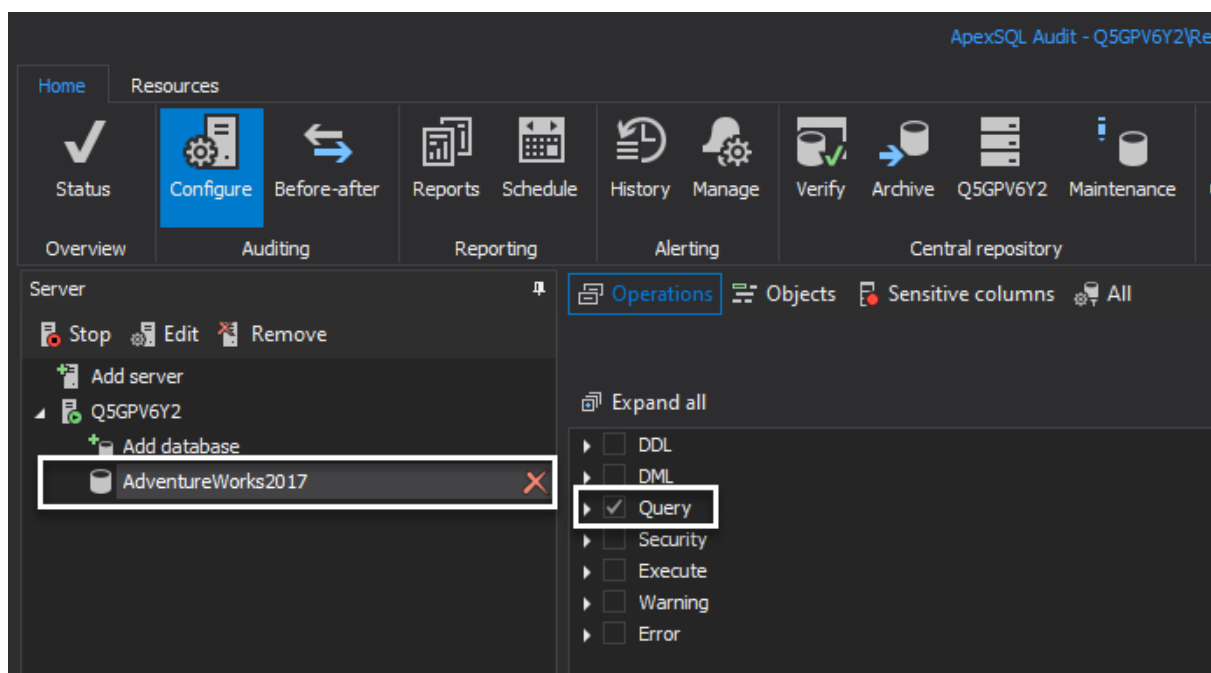
Creating a database audit trail can be achieved via multiple different SQL Server techniques, that are explained in this [SQL Server database auditing techniques](#) guide, and for this article, we will be focusing the out-of-the-box solution to track sensitive data access via ApexSQL Audit, as a proper and easy to configure auditing tool for this task.

Nikhil Yadav (nikhil27rock@gmail.com)

Although sensitive data auditing has been already introduced in the Discover section of this article, we fell short to broadly explain how to perform the configuration steps and demonstrate the auditing trail details. Therefore, here is a quick guide on how to track sensitive data access and create reports.

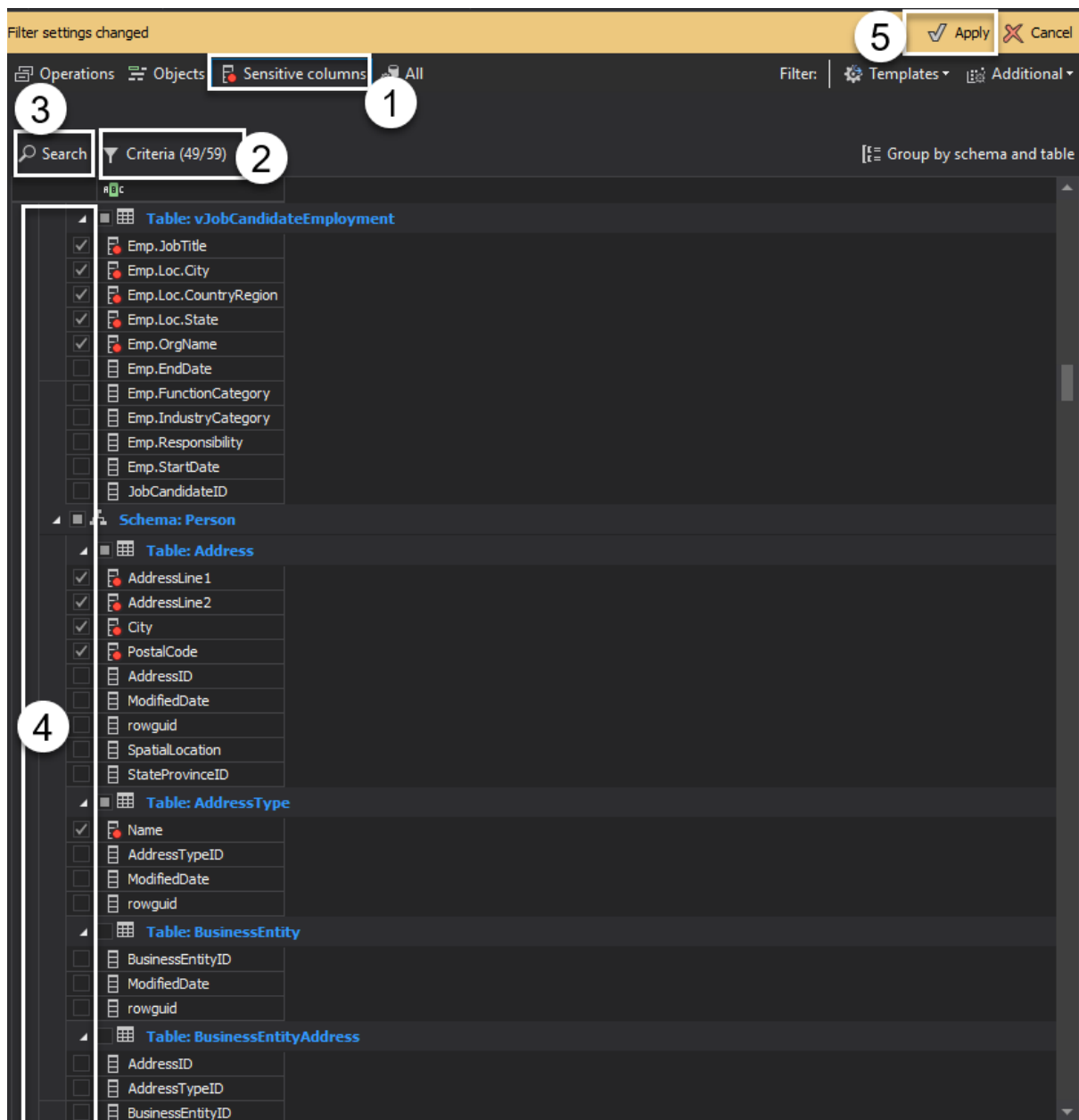
Configure database auditing

SQL Server database holding sensitive data should be added to the auditing list first, and the Query operations are audited on the database so the data access against sensitive rows can be captured:



The next step is to switch to the Sensitive columns pane and perform the following steps to configure sensitive data access auditing on the rows holding such information:

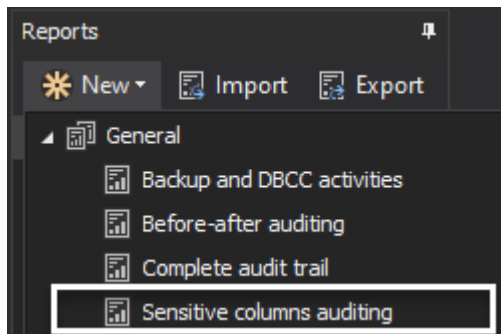
1. Go to sensitive columns pane
2. Define search criteria
3. Run search
4. Columns that matched search criteria are automatically marked as sensitive and pre-selected in a result grid, add or remove certain columns
5. Hit apply changes



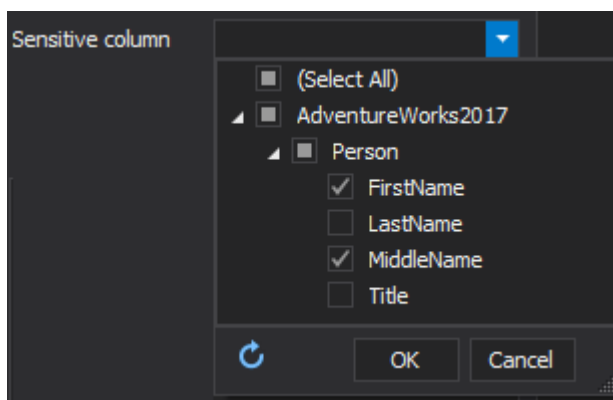
With this, sensitive data configuration is complete, and the audited data will be available in the audit trail reports.

Creating a sensitive data access report

The main purpose of employing database auditing is to create and run audit reports. ApexSQL Audit provides a various number of pre-defined reporting templates, including Sensitive columns auditing to reconstruct the audit log information relating sensitive data access only:



Sensitive column reports filters can be further customized to reconstruct auditing information per desired specifications, including this special control to select any specific column:



Once the filter customization is complete, the audit trail report can be quickly previewed in the application overview grid. The same output can be also exported into multiple file-formats on-demand, or via the scheduled jobs:

Preview

Generate

All days

Columns

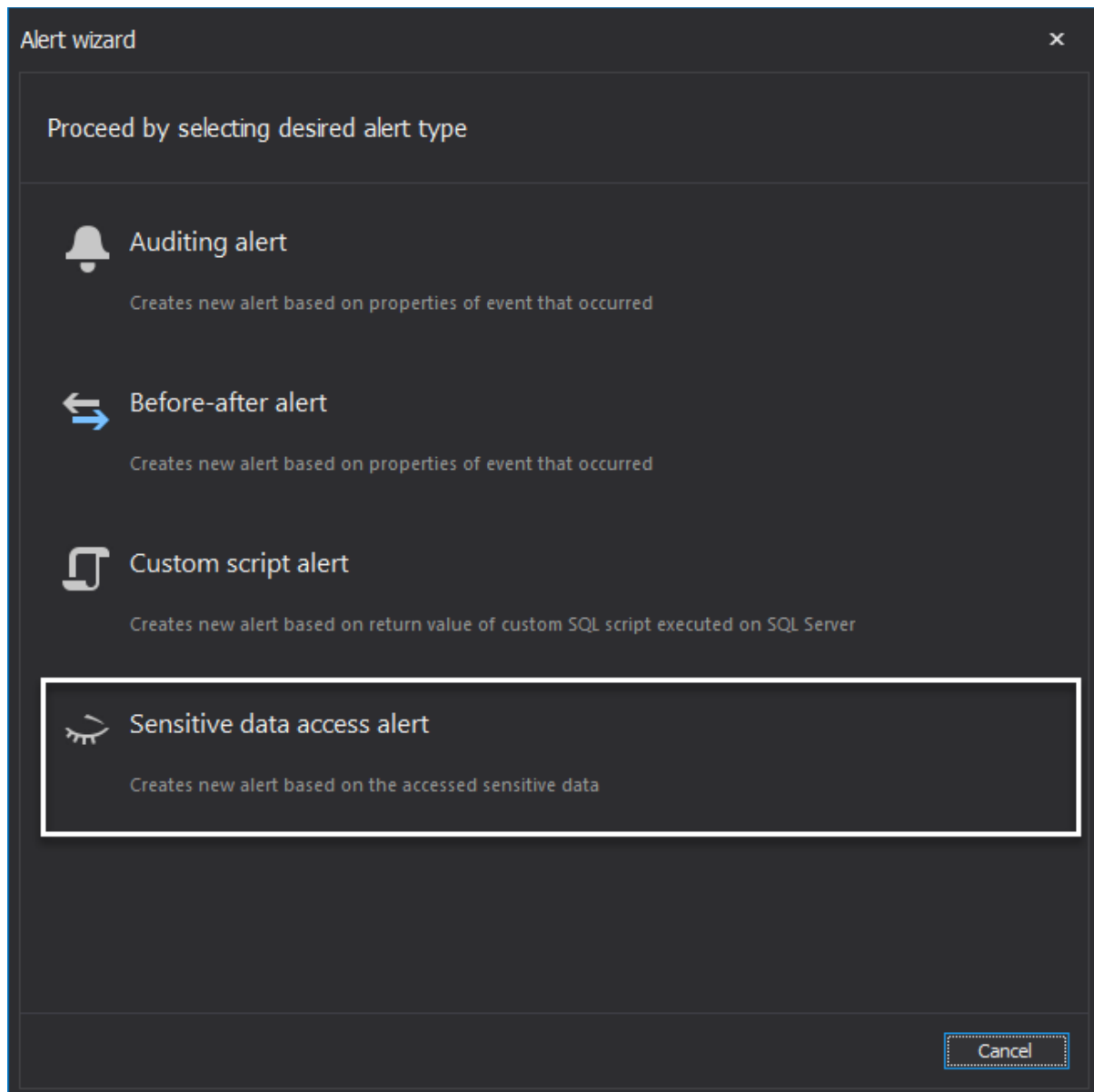
Date	Server	Database	Login	Application	Client host	Schema	Object	Operation
07/28/2020 11:13:19.610 PM	Q5GPV6Y2	AdventureWorks2017	PROD\RKuc	Microsoft SQL Server Management Studio - Query	Q5GPV6Y2	Purchasing	vVendorWithAddresses	Select
Accessed column(s)								
Addressline1								
Addressline2								
Name								
AddressType								
City								
StateProvinceName								
PostalCode								
CountryRegionName								
07/28/2020 11:11:40.283 PM	Q5GPV6Y2	AdventureWorks2017	PROD\RKuc	Microsoft SQL Server Management Studio - Query	Q5GPV6Y2	Person	Address	Select
Accessed column(s)								
Addressline1								
Addressline2								
07/28/2020 11:10:27.850 PM	Q5GPV6Y2	AdventureWorks2017	PROD\RKuc	Microsoft SQL Server Management Studio - Query	Q5GPV6Y2	Person	Password	Select
Accessed column(s)								
PasswordHash								
PasswordSalt								

Creating sensitive data access alerts

Nikhil Yadav (nikhil27rock@gmail.com)

Having a mechanism to work around the clock and validate database activity is the long arm of control measures to help identify any uncertainty in the environment. With the alerting mechanism in the database auditing solution, any control violation can be identified proactively and consistently. ApexSQL Audit provides this capability via real-time alerting to raise awareness about any specific event via e-mail notification.

Specific columns access alert can be easily set via the dedicated alert type for Sensitive data access alert:



ApexSQL Audit provides the capability to identify any specification and let you know about it. So, let's set up an alert rule to trigger a notification when any user apart from a group of users should make transactions against certain columns:

Nikhil Yadav (nikhil27rock@gmail.com)

Alert wizard

New sensitive data access alert

Trigger a High severity alert for the following server
Q5GPV6Y2

Sensitive columns:
AdventureWorks2017.Person.Person.FirstName
AdventureWorks2017.Person.Person.LastName

Alert condition
login name is not:
ApexSQLAuditDemo
PROD\RKuc

Action
High alert triggered

Send alert to the following addresses
To: DBA@Quest.com

Write alert report to Windows event log

Alert name: New sensitive data access alert

< Back Finish Cancel

With this, we are about to complete the circle of controlling and monitoring sensitive data access in the SQL Server environment. Employing database auditing to log, and review data, or raise alerts will significantly improve revision experience. To learn more about details specifics on how to create and run reports or alerts, consult this [Creating sensitive data reports and alerts article](#).

Summary

Building a safe and sound strategy for control assessment and sensitive data management requires enough planning ahead. This guide was intended to help throughout the complete cycle while identifying the core techniques and how database auditing can help cover each pillar of this strategy. Over the course, every organization is challenged with changes in data movement and how it is processed, managed, and controlled. This cyclic approach is meant

Nikhil Yadav (nikhil27rock@gmail.com)

to address the challenge by repeating this act with positive consequences, Discover – Manage – Monitor.

Big Data

Big Data is an ever-changing term – but mainly describes large amounts of data typically stored in either Hadoop data lakes or NoSQL data stores. Big Data is defined by the 5 Vs:

1. **Volume** – the amount of data from various sources
2. **Velocity** – the speed of data coming in
3. **Variety** – types of data: structured, semi-structured, unstructured
4. **Veracity** – the extent to which the data is trustworthy
5. **Value** – ensure insights from the data have value beyond the underlying cost
6. Big Data is growing at a rapid pace. According to IBM, 90% of the world's data has been created in the past 2 years. And with Big Data comes bad data.
7. And this is important because [C-level executives are using BI & Analytics](#) to make critical business decisions with the assumption that the underlying data is fine.
8. [We know it is not.](#)

Big Data Testing Issues

9. Typical testing around traditional data warehouses or databases revolve around structured data and using SQL to accomplish the testing.
10. Big Data testing is completely different. Big Data deals with not only structured data, but also semi-structured and unstructured data and typically relies on HQL (for Hadoop), relegating the 2 main methods, [Sampling](#) (also known as “stare and compare”) and [Minus Queries](#), unusable.

QuerySurge will help you:

- [Continuously detect data issues](#) in the delivery pipeline
- Dramatically increase [data validation coverage](#)
- [Leverage analytics](#) to optimize your critical data
- Improve your [data quality at speed](#)
- Provide a huge [ROI](#)

QuerySurge Features

Browse through the key features of QuerySurge. Navigate to the topic of your interest on the left, and the specific Feature details will show up on the right.

Supported Vendors and Technologies

Nikhil Yadav (nikhil27rock@gmail.com)

QuerySurge supports all of the data stores below as either a source or target.

- Amazon **Redshift**, **DynamoDB**, **Simple Storage Service (S3)**, **Athena**
- **Apache Hadoop/Hive/Spark/Kafka**
- Azure **Analysis Services**, **Data Lake Storage**, **Blob Storage**, **SQL Data Warehouse**, **SQL Database**
- **EXASOL**
- **Cassandra**
- Confluent **KSQL**
- Couchbase
- **Cloudera**
- **Databricks in Azure**
- **Dremio**
- **Flat Files** (**delimited** and **fixed-width**)
- **Google BigQuery**
- **Hortonworks**
- HP Tandem
- IBM (**DashDB**, **BigInsights**, **DB2**, **Netezza**, **Informix**, **Cloudant**, **Cognos Analytics**)
- **JSON**
- **Mainframe**
- MapR
- Microsoft (Azure Synapse Analytics, **SQL Server**, **PDW**, **SSAS**, **Access**, **Excel**)
- **MicroStrategy**
- **MongoDB**
- Oracle (**Oracle db**, **MySQL**, **Exadata**)
- Pivotal **GreenPlum**
- **PostgreSQL**
- **Salesforce**
- SAP (**HANA**, **IQ**, **ASE**, **SQL Anywhere**, **Business Objects**)
- **Sharepoint**
- **Snowflake**
- **Tableau**
- **Teradata**, **Aster**
- **Vertica**
- **Workday**
- **XML**