IBM QRadar
Version 7.3.0

Security Technical Implementation Guide (STIG)

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 15.

Product information

This document applies to IBM® QRadar® Security Intelligence Platform V7.3.0 and subsequent releases unless superseded by an updated version of this document.

Contents

About this STIG for QRadar guide

This documentation includes the requirements and procedures for configuring STIG on IBM Security QRadar.

Intended audience
The intended audience for this guide is system administrators or developers who are configuring STIG for IBM Security QRadar.

Technical documentation

To find IBM Security QRadar product documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. Overview of STIG for QRadar installations

This Security Technical Implementation Guide (STIG) provides the configuration standards and steps that are required for IBM Security QRadar deployments to achieve the level of security that is required to operate in US Department of Defense (DoD) computer networks.

This STIG implementation follows IBM secure engineering practices.

What systems can you run STIG scripts on?

You can run STIG scripts on QRadar All-in-One consoles. You can also run STIG scripts on Event Processors and Flow Processors, but you must use the expert guidance of your IBM Security QRadar Client Technical Professional (CTP) or IBM QRadar Product Professional Services to complete the task.

IBM Security QRadar is working to support running STIG scripts on the following products, but they are not currently supported:

- IBM QRadar Network Insights
- IBM Security QRadar Incident Forensics
- IBM QRadar Network Packet Capture
- IBM Security QRadar Packet Capture
- QRadar Packet Capture Data Nodes
- IBM Security QRadar Risk Manager
- IBM Security QRadar Master Console
- App Nodes

Exceptions to STIG compliance

For operational and performance reasons, full-disk encryption, SELinux (Security-Enhanced Linux), and patch maintenance are intentionally excluded from the hardening procedures for full STIG compliance.

Full-disk encryption

The Red Hat Enterprise Linux 7 Security Technical Implementation Guide (STIG) (beta) states that you must enable *LUKS* (Linux Unified Key Setup-on-disk-format), which is full-disk encryption. However, the performance degradation that is experienced in a QRadar deployment prohibits this full-disk encryption. The suggested solution is to maintain all QRadar hosts in a physically-secured environment.

SELinux considerations

If you enable SELinux in enforcement mode, the performance of QRadar is significantly impacted. An alternative template for QRadar hosts is not available.

You must protect your privileged user passwords so that access to the operating system is restricted.

Software maintenance

Software fixes or updates for QRadar hosts are provided only by IBM, whether Red Hat Enterprise Linux is installed separately or not. You must disable Red Hat Enterprise Linux subscription feeds, and all RPM updates must be provided only by IBM. IBM regularly provides software fixes and updates for product defects and known vulnerabilities within QRadar and Red Hat Enterprise Linux.

Root logins

When you run STIG on an All-in-One appliance, you can't use the SSH root account to log in remotely to the QRadar Console.

SSH access control

IP (Internet Protocol) based access controls for SSH connections are applied to managed hosts but not to Consoles.

Note: Use iptables rather than SSH configuration to restrict SSH access.

See the *IBM Security QRadar Administration Guide* for information about creating iptables rules.

Routing and Bridging

Docker containers that run on QRadar hosts use bridged interfaces for connecting and routing to the host. You can't disable forwarding (routing) on a QRadar host because it might block communication with the containers. To limit the risk with forwarding, use iptables firewall filtering instead.

FTP

An FTP server package (vsftpd) is installed on QRadar hosts but is unavailable on all QRadar hosts except for QRadar Incident Forensics hosts.

When the FTP server package is enabled it uses TLS authentication and chroot to restrict access. The FTP daemon only runs when QRadar Incident Forensics is being used.

Note: You can remove the FTP package but it might impact future product upgrades and cause them to fail.

Chapter 2. Prerequisites for STIG implementation

You must prepare your IBM Security QRadar setup before you implement STIG.

Hardware

All QRadar hardware that is required in the deployment must be available and ready to configure.

Software

The hardening script is included in the QRadar ISO image. You can install RHEL 7 separately, but you don't have to because QRadar 7.3 comes with the pre-requisite RPMs installed, suitable partitioning, and uses LVM.

The only time you might pre-install RHEL 7 is when you want to uses Full Disk Encryption but it's not supported.

Chapter 3. Installing QRadar in a STIG environment overview

This Security Technical Implementation Guide (STIG) provides guidance for implementing security standards for IBM Security QRadar deployments that meet the requirements set by the Defense Information Systems Agency (DISA). Hardening of the operating system and QRadar hosts are part of making QRadar deployments more secure.

About this task

Use STIG for highly secure environments, such as the federal government. The procedures in this guide are not suitable for every QRadar deployment.

Note: Before you run the STIG scripts on a managed host, you must add the managed host to your QRadar deployment and deploy a full configuration. When you run the STIG scripts, secure key authentication replaces the requirement for root passwords between the Console and the managed host.

You must complete the following procedures to make QRadar STIG-compliant:

Procedure

1. Install the QRadar 7.3 ISO image by following the steps that are specified in the *IBM Security QRadar Installation Guide*.

   If you choose to

   do a software install and install RHEL separately, then you must follow the partitioning guidelines in the *IBM Security QRadar Installation Guide*.
2. Create a non-root user.
3. Run scripts that automate hardening of the operating system.
4. Edit QRadar scripts.
5. Change the boot loader configuration.

Creating a non-root user in a STIG-compliant environment

You can't log in remotely as the root user in a STIG-compliant environment. On each host in the QRadar deployment, create a non-root user who has **sudo** access and choose a non-root user name such as stiguser.

Procedure

1. To create the non-root user, type the following commands:

   ```
   useradd -c 'Admin User' -d /home/stiguser -m -s /bin/bash stiguser
   ```

   ```
   passwd stiguser
   ```

   The password must follow these guidelines:

   - Consist of 15 or more characters.
   - Not repeat the same character consecutively more than two times.
   - Not repeat the same character type consecutively more than two times.
   - Have at least one uppercase character.
   - Have at least one numerical character.
   - Have at least one special character.

Tip: These new password requirements are enforced when the STIG script is run. If your root password doesn't meet these requirements, you can change it now.

2. Edit the `/etc/sudoers` file and at the end of the file, type the following line:

   ```
   stiguser ALL=(ALL) ALL
   ```

   Note: It is conventional to use tabs for white space but it's not a requirement; for example:

   ```
   stiguser ALL=(ALL) ALL
   ```

   Use the # symbol to comment out any lines that contain `NOPASSWD`.

   Tip: If you use the Vim text editor, type **`:/NOPASSWD`** in command mode to search for any instances of `NOPASSWD`.

3. Verify that the new user can log in from a remote host and use the **sudo** command to become a root user.

   For example, log in to the IBM Security QRadar as stiguser by using an SSH client such as PuTTY, and then run a command by using **sudo**; for example, **`sudo cat /etc/shadow`**.

Running the hardening script on the Console

To help secure the system, you must run hardening scripts on the IBM Security QRadar Console.

Before you begin

Before you run the hardening script, verify that the stiguser can log in remotely.

Procedure

1. Go to the STIG directory by typing the following command:

   ```
   cd /opt/qradar/util/stig
   ```

2. Run the STIG hardening script by typing the following command:

   ```
   ./stig_harden.sh -h
   ```

   Type `yes` at the following prompt: **Do you want to continue (yes/no)?**

   Note: You must run the script only once.

3. Replace the `ssl.conf` and `httpd.conf` files in `/etc/httpd/conf` with the same files from the `/store/STIG directory`.

   a) Copy the `/store/STIG/orig-files` file to `/etc/httpd/conf/httpd.conf`.

   b) Copy the `/store/STIG/orig-files` file to `/etc/httpd/conf.d/ssl.conf`.

   Note: You are overwriting the `http.conf` and `ssl.conf` files in the `/etc/httpd/conf` directory. These files aren't changed when the script is run.

4. Restart the QRadar appliance.

5. Verify that the `stiguser` can log in remotely at the same time that you (as administrator) are logged in as a root user.

   If you are hardening a managed host, change the root user's password to meet the password requirements. Ensure that the root authentication works locally.

Editing scripts to configure QRadar in STIG environments

Extra configuration tasks, such as configuring the mail server, disabling the DHCP client, updating iptables, and changing the backup log directory location are required when you configure QRadar in STIG environments.

Procedure

1. To ensure that the mail server on each host is listening on local interfaces:
   a) Make a backup copy of the `/etc/postfix/main.cf` file.
   b) Edit the `/etc/postfix/main.cf` file and verify that the `inet_interfaces` line is similar to one of the following examples:
      - `inet_interfaces = localhost`.
      - `inet_interfaces = loopback-only`.
   c) Restart postfix by typing the following command:

      ```
      systemctl restart postfix
      ```
2. Disable the DHCP client by editing the `/etc/sysconfig/network-scripts/ ifcfg*` files:
   a) Type the following command:

      ```
      grep –i BOOTPROTO /etc/sysconfig/network-scripts/ ifcfg*
      ```
   b) For each interface configuration file that is returned, change the **BOOTPROTO** value to **none** if this value is not equal to **`static`** or **none**. In the following example the **BOOTPROTO** value equals **none**.

      Example:

      ```
      DEVICE=ens192
      ONBOOT=yes
      BOOTPROTO=none
      IPADDR=192.168.122.254
      NETMASK=255.255.255.0
      ```
3. Change `iptables` and set the default INPUT policy to *DROP*:
   a) Make a backup copy of the `/opt/qradar/bin/iptables_update.pl` file.
   b) Edit the `/opt/qradar/bin/iptables_update.pl` file and change all instances of `INPUT ACCEPT [0:0]` to `INPUT DROP [0:0]`.
   c) Run the `/opt/qradar/bin/iptables_update.pl` script.
4. Add the following line at the end of the `/etc/hosts.allow` file on the QRadar Console:

   ```
   time: ALL
   ```
5. Change the backup log directory:
   a) Search for the `/var/log/backup.log` log file and if it exists, move the file to `/store/LOGS`.

      Note: The `/var/log/backup.log` does not exist on a fresh install.
   b) Make a backup copy of the `/opt/qradar/bin/backup.sh` file.
   c) Edit the `/opt/qradar/bin/backup.sh` file and replace the

      ```
      InitLog @syslog:local1.info || ErrorExit 'Failed to initialize logging'
      ```

      line in the `/opt/qradar/bin/backup.sh` file with the following line:

      ```
      InitLog /store/LOGS/$(basename ${0} .sh).log || ErrorExit 'Failed to initialize logging'
      ```

      .
6. To disable packet forwarding on a host that is not a QRadar Console:
   a) Run the following script to disable forwarding on a host that is not a QRadar Console:

```
sysctl -w net.ipv4.ip_forward=0
```

b) Edit the `/etc/sysctl.conf` file to add the `net.ipv4.ip_forward = 0` line.

7. Create an AIDE baseline, schedule integrity checks, and create the baseline and schedule updates.

a) To check for the existence of `prelink`, type the following command:

```
rpm -qa | grep prelink
```

If nothing is returned, skip step b.

b) If results for `prelink` are returned in step a, run the following command:

```
/usr/sbin/prelink -ua
```

c) As root user, initialize the AIDE database by typing:

```
aide --init
```

d) Create a cron script in `/etc/cron.d` to enable the following `aide --update`:

```
mv -f /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz ; aide --
update
```

e) Run the `aide --update` after you run a QRadar deployment action.

The content in the monitored fields changes when configuration changes are made after a deployment.

8. To configure **audit logging** forwarding to a remote log server:

a) In the `/opt/qradar/syslog-ng/syslog-ng.conf.default` file, change the following entry from:

```
# local4.info                                           -/var/log/audit/audit.log
filter local4_info { facility(local4) and level(info..emerg) and not match("Token: Local Health Console"
value("MESSAGE")); };
destination audit  { file("/var/log/audit/audit.log" perm(0600) create_dirs(yes) flush_lines(20) flush_timeout(500)); };

log { source(local); filter(local4_info); destination(audit); };
```

to:

```
# local4.info                                           -/var/log/audit/audit.log
filter local4_info { facility(local4) and level(info..emerg) and not match("Token: Local Health Console"
value("MESSAGE")); };
destination audit  { file("/var/log/audit/audit.log" perm(0600) create_dirs(yes) flush_lines(20) flush_timeout(500)); };
destination remote_audit { udp("$$LOGHOST$$" port(514)); };
log { source(local); filter(local4_info); destination(audit); };
log { source(local); filter(local4_info); destination(remote_audit); };
```

b) Replace $$LOGHOST$$ with the IP address of the appropriate log host.

Changing the boot loader configuration

Change the GRUB 2 boot loader settings to configure the non-root user for STIG environments and other settings. Update the GRUB 2 boot loader configuration on the QRadar Console, event processors, and flow processors.

About this task

The `stig_harden.sh` sets `audit=1` in the `/etc/default/grub` file.

Update the GRUB 2 configuration for the change to be effective.

Procedure

1. Type `tar -cvf /root/grub2backup.tar /etc/grub.d /etc/default/grub /boot/grub2` to back up of the following GRUB 2 configuration files and directories:
   - `/etc/grub.d`
   - `/etc/default/grub and /boot/grub2`

2. Run the following script to generate a password hash for the boot loader.

   `grub2-mkpasswd-pbkdf2`

   Note the hash value that is generated, and use the hash value output to replace the hash content (example) in step 3.

   Tip: You can copy and paste the generated hash value if you complete this step remotely by using the stiguser user account.

3. Edit the `/etc/grub2.cfg` file, by typing the following two lines:

   `set superusers=stiguser` and

   `password_pbkdf2 stiguser` after the

   ### END /etc/grub.d/00_header ### line, and then paste the hash value content from step 2.

   Here's an example:

```
### END /etc/grub.d/00_header ###
set superusers=stiguser
password_pbkdf2 stiguser
 1 grub.pbkdf2.sha512.10000.51A734C16CD93009EED3814937CCBABAF
70256B5EB67BE6B6D96138A110B3092722248605923588F143375E09149520ADE32
5EB4791DA08C74F0E48A2A1CD3F8.D1B528BD41790DAFF9479A511FD95EF03B4F4A
583EF6DA53AA2DFE10941A028F15AA9ADEEEE0E3398F5734516655820C836BBBA86
5911282D326C5B7EA2FEC1A 2
### BEGIN /etc/grub.d/10_linux ###
```

   You insert the hash value between 1 and 2, which follows the `set superusers=stiguser` and `password_pbkdf2 stiguser` lines.

   For example,

```
### END /etc/grub.d/00_header ###
set superusers=stiguser
password_pbkdf2 stiguser
<hash_value_content...>
### BEGIN /etc/grub.d/10_linux ###
```

   Note: The hash value content line that starts with `grub.pbkdf2` is one continuous line.

4. In the `/boot/grub2/grub.cfg` file, edit every line that begins with `menuentry` so that `--users` is followed by `stiguser`.

   Here's an example:

```
### BEGIN /etc/grub.d/10_linux
### menuentry 'Red Hat Enterprise Linux Server'
--class gnu-linux --class gnu --class os --users stiguser
$menuentry_id_option 'gnulinux-simple-f804409d-9e87-4e19-a321-a26b55a66fd9'
{ load_video set gfxpayload=keep
```

   Tip: If you use the Vim text editor, type **`:/menuentry`** to search for any instances of `menuentry`.

   Note: If `--class os` is followed by `--unrestricted`, replace `--unrestricted` with `--users stiguser`.

Chapter 4. Post-installation checks

Post-installation checks are required to complete your STIG compliance.

Note: If you've install QRadar and RHEL from the QRadar ISO image, the following checks might not be necessary.

Passwords restricted to 1-day minimum lifetime

Type the following command to check for any violations:

```
awk -F: '$4 >= 1 {print $1}' /etc/shadow
```

You must change the password-restriction setting for any non-system accounts or non-user accounts that are displayed.

Passwords restricted to 60-day maximum lifetime

Type the following command to check for any violations:

```
awk -F: '$5 >= 1 {print $1}' /etc/shadow
```

You must change the password-restriction setting for any non-system accounts or non-user accounts that are displayed.

Duplicate user IDs (UID)

Type the following command to check for duplicate user IDs:

```
pwck -rq
```

Accounts that are displayed are in violation of this rule.

Chapter 5. STIG notes

Review vulnerabilities updates and software updates regularly to make sure that your environment is current.

Vulnerabilities

Some false positives in QRadar are caused by software banners such as Apache that might display older versions than the installed version. Vulnerability scans often report false positives for critical software such as Apache, and OpenSSH.

Upgrading QRadar software

Before you upgrade QRadar software on a STIG hardened system in a production environment, ensure that you have a full backup that is up to date, and test software upgrades in a pre-production environment.

If you can't test a software upgrade in a pre-production environment, and you want to be fully protected before you upgrade QRadar software on a STIG hardened system, back up your data and system configuration and then take the following steps:

1. Reinstall QRadar and RHEL software.
2. Install software fixes.
3. Restore the data and system configuration.
4. Run the STIG scripts.

Maintenance in STIG environments

QRadar changes or upgrades might undo the configuration that you made, as part of the STIG hardening procedure.

Some files or scripts in the `/opt/qradar` directory are impacted by a QRadar software update or upgrade. The logging configuration and SSHD configuration are also impacted. Restore the hardening configuration by rerunning the hardening scripts, and then verifying that the manual changes that you made are implemented.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations

that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr