IBM Disconnected Log Collector
Version 1.0.0

IBM Disconnected Log Collector guide

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 11.

Product information

This document applies to IBM® Disconnected Log Collector V1.0.0-1 and subsequent releases unless superseded by an updated version of this document.

Contents

Chapter 1. IBM Disconnected Log Collector

Disconnected Log Collector is free software that accepts events from a limited set of log sources and sends them to an IBM QRadar® deployment. Disconnected Log Collector is compatible with QRadar V7.3.1 and higher.

Currently, Disconnected Log Collector accepts UDP syslog and TCP syslog source protocols.

Disconnected Log Collector sends events to a QRadar deployment by using the User Datagram Protocol (UDP) or by using Transport Layer Security over the Transmission Control Protocol (TLS over TCP). When Disconnected Log Collector uses TLS over TCP, it buffers incoming events during times when it's disconnected from QRadar and sends them when the connection is restored. Buffer capacity can be configured, and is limited by the available disk space. Disconnected Log Collector doesn't impose any events-per-second limit.

You can use as many Disconnected Log Collector instances as you need in your QRadar environment.

Business scenarios for using Disconnected Log Collector

Disconnected Log Collector is suitable for a range of business scenarios:

Secured network zones
In high-security unidirectional networks (also known as *data diodes*), Disconnected Log Collector can use the connectionless UDP protocol to send events to QRadar. Disconnected Log Collector instances can be daisy-chained over multiple secured network zones.

Managed security service providers (MSSPs)
Disconnected Log Collector can be installed on small to medium-sized customer sites and doesn't rely on a virtual private network (VPN) to send events to the MSSP. Disconnected Log Collector simplifies administration because each instance clearly belongs to a particular customer domain.

Multi-location businesses
In large retailers and other multi-location businesses, each location typically generates only a small number of events per second that doesn't justify the cost of a 15xx Event Collector appliance. Disconnected Log Collector can be installed on a cost-effective Linux computer or virtual machine, where it can collect and send events to the central security infrastructure.

IBM QRadar on Cloud deployments
For businesses that track only events (not flows or vulnerability scans), Disconnected Log Collector is a lightweight alternative to installing a Data Gateway managed host and doesn't rely on a VPN to send events to QRadar on Cloud.

System requirements for IBM Disconnected Log Collector

Disconnected Log Collector is compatible with QRadar V7.3.1 and higher, and must be installed on a computer or virtual machine (VM) that meets the following requirements.

System hardware

Table 1: System hardware requirements for Disconnected Log Collector

Requirement	Description
Memory (RAM)	2 GB or more of free RAM.
Disk space	52 GB or more of free disk space.

Table 1: System hardware requirements for Disconnected Log Collector (continued)

Requirement	Description
Processor	Optimal: 2 CPU cores Minimum: 1 CPU core
Network adapter	One or more network adapters.

Operating system

Disconnected Log Collector requires the Red Hat Enterprise Linux (RHEL) or CentOS Linux V7.x operating system.

Disconnected Log Collector creates its own user account, named **dlc**. It doesn't require any other user accounts on the system.

For more information about installing and configuring RHEL or CentOS Linux, see the RHEL documentation (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/).

Firewall ports

Disconnected Log Collector requires port 1514 (TCP and UDP) to be available and not blocked.

Java

Disconnected Log Collector requires IBM SDK, Java™ Technology Edition, Version 8, 64-bit. The download location is https://developer.ibm.com/javasdk/downloads/sdk8/. Choose the Linux *InstallAnywhere as root* installation package that's right for your system hardware.

Before installation, adjust the permissions on the downloaded binary file by using the `chmod a+x` `<ibm_sdk_java_install>.bin` command.

Use the default installation location, which is `/opt/ibm/java-x86_64-80/`.

For information about installing and configuring IBM SDK, Java Technology Edition, Version 8, see the SDK User Guide (ibm.com/support/knowledgecenter/en/SSYKE2_8.0.0).

Installing IBM Disconnected Log Collector

Install Disconnected Log Collector on a computer or virtual machine that meets all the system requirements. You can install only one instance of Disconnected Log Collector per computer or VM.

Before you begin

Download Disconnected Log Collector from IBM Fix Central (ibm.com/support/fixcentral/).

Ensure that all system requirements are met and that IBM SDK, Java Technology Edition is installed.

Procedure

1. Log in to the Disconnected Log Collector computer or VM as the root user.
2. Copy the Disconnected Log Collector RPM file to `/tmp` or your preferred location.
3. Install Disconnected Log Collector by using the following command:

   ```
   yum -y install /tmp/<dlc_installer_file>.rpm
   ```

4. After the installation is finished, run the following command and check for a `status:running` message to confirm that the installation was successful and Disconnected Log Collector is running:

   ```
   systemctl status dlc
   ```

Results

By default, Disconnected Log Collector uses the User Datagram Protocol (UDP) to send log events. Because you still must configure a connection to IBM QRadar, any incoming events are sent only to the local computer.

Opening required ports in the Linux firewall

IBM Disconnected Log Collector requires several ports to be open in the Linux firewall so that it can receive incoming log sources and communicate with IBM QRadar. Port forwarding is also required so that you can use Disconnected Log Collector without needing root privileges.

About this task

On communication protocols such as UDP and TCP, ports 1 - 1023 are *privileged* and require a process to be running with root privileges. Disconnected Log Collector uses port 514 to receive incoming log sources. Therefore, to use Disconnected Log Collector without needing root privileges, you must forward port 514 to a *non-privileged* port that is 1024 or greater. For convenience, the default target port for forwarding is 1514.

Procedure

1. Log in to the Disconnected Log Collector computer or VM as the root user.
2. Open ports by using the following commands:

```
firewall-cmd --list-all
firewall-cmd --zone=public --add-port=514/udp --permanent
firewall-cmd --zone=public --add-port=514/tcp --permanent
```

3. Forward ports by using the following commands:

```
firewall-cmd --zone=public --add-forward-port=port=514:proto=tcp:toport=1514 --permanent
firewall-cmd --zone=public --add-forward-port=port=514:proto=udp:toport=1514 --permanent
```

   Important: The default target port for forwarding is 1514. If you specify a different target port in the `dlc.xml` configuration file, you must substitute it in the port forwarding commands. The target port number must be 1024 or greater.

4. Reload the firewall by using the following command:

```
firewall-cmd --reload
```

Changing the IBM QRadar server destination port

By default, IBM Disconnected Log Collector sends events to QRadar server port 32500. You can change the destination port if 32500 is not available on the QRadar server.

About this task

The destination port must match the **Listen Port** that is specified in the Disconnected Log Collector protocol on the QRadar system. For more information, see "Adding IBM Disconnected Log Collector as a log source in IBM QRadar" on page 8.

Important: For IBM QRadar on Cloud, the destination port must not be changed from 32500.

Procedure

1. Log in to the Disconnected Log Collector computer or VM as the root user.
2. Open the `/opt/ibm/si/services/dlc/conf/config.json` file in a text editor.

3. In the **destination.port** parameter, enter the listening port for the Event Collector, Event Processor, or QRadar Console that will receive events from the Disconnected Log Collector instance. For example:

```
'destination.port':'32501'
```

4. Save and close the `config.json` file.
5. Restart Disconnected Log Collector by using the following command:

```
systemctl restart dlc
```

Setting up UDP communication with IBM QRadar

User Datagram Protocol (UDP) is a connectionless protocol that is suitable for one-way communication, such as in unidirectional networks (also known as *data diodes*). UDP is susceptible to spoofing and should be used only in isolated, secure networks. UDP is the default protocol that IBM Disconnected Log Collector uses to send event logs to an IBM QRadar deployment.

About this task

Event log data is buffered only during moments when the incoming events-per-second rate exceeds the computer's ability to relay the information in real time. Event log data is not buffered if connection is lost between Disconnected Log Collector and QRadar.

Procedure

1. Log in to the Disconnected Log Collector computer or VM as the root user.
2. Open the `/opt/ibm/si/services/dlc/conf/config.json` file in a text editor.
3. In the **destination.type** parameter, enter UDP (the default):

```
'destination.type': 'UDP'
```

4. In the **destination.ip** parameter, enter the IP address for the Event Collector, Event Processor, or QRadar Console that will receive events from the Disconnected Log Collector instance. For example:

```
'destination.ip':'192.168.0.2'
```

5. Save and close the `config.json` file.
6. Restart Disconnected Log Collector by using the following command:

```
systemctl restart dlc
```

What to do next

Now you're ready to add IBM Disconnected Log Collector as a log source in QRadar. For more information, see "Adding IBM Disconnected Log Collector as a log source in IBM QRadar" on page 8.

Setting up certificate-based authentication on IBM Disconnected Log Collector

In TLS over TCP communication between Disconnected Log Collector and IBM QRadar, certificate-based communication is used to establish a *chain of trust* in which hardware and software is validated from the end entity to the root certificate.

Before you begin

You must have a root certificate that was issued by a trusted certificate authority (CA). Typically, you use the same root certificate on the Disconnected Log Collector and QRadar computers. Ensure that the root certificate has a meaningful name, such as `root-ca.cer`.

About this task

Every certificate has a validity period (a date range) during which it can be used to establish secure communications. After the validity period ends, the certificate expires and must be replaced.

Procedure

1. Log in to the Disconnected Log Collector computer or VM as the root user.
2. Copy the root certificate to `/etc/pki/ca-trust/source/anchors` and run the following command to update the default truststore:

   ```
   update-ca-trust
   ```

3. Generate a client certificate signing request (CSR) by using the following command:

   ```
   /opt/ibm/si/services/dlc/current/script/generateCertificate.sh -csr (-2k | -4k)
   <your_organization_name> <your_organizational_unit_name>
   ```

   Choose the key size for the certificate according to the requirements of your organization. `-2k` Represents 2048 bits; `-4k` represents 4096 bits.

   For example:

   ```
   /opt/ibm/si/services/dlc/current/script/generateCertificate.sh -csr -2k IBM IBMSupport
   ```

   A client CSR file is saved as `/opt/ibm/si/services/dlc/keystore/<UUID>/dlc-client.csr`, where UUID is an identifier that is unique to the Disconnected Log Collector instance.
4. Submit the CSR to your internal or commercial certificate authority for signing, according to their instructions. The procedure might involve opening the CSR file and copying a block of encoded text that is contained between BEGIN and END markers.
5. Copy the returned client certificate to `/tmp` or your preferred location.
6. Convert the client certificate to PKCS#12 format by using the following command, and choose a secure password when prompted:

   ```
   /opt/ibm/si/services/dlc/current/script/generateCertificate.sh -p12
   /tmp/<signed_certificate_file_name>
   ```

   A generated personal exchange format (PFX) file is saved as `/opt/ibm/si/services/dlc/keystore/dlc-client.pfx` and the required PFX information is stored in the `/opt/ibm/si/services/dlc/conf/config.json` file.
7. Restart Disconnected Log Collector by using the following command:

   ```
   systemctl restart dlc
   ```

What to do next

Make note of the UUID identifier that is unique to the Disconnected Log Collector instance. The identifier is the `/opt/ibm/si/services/dlc/keystore/<UUID>` folder name. You'll need the UUID when you configure the Disconnected Log Collector protocol in QRadar. For more information, see "Adding IBM Disconnected Log Collector as a log source in IBM QRadar" on page 8.

Setting up certificate-based authentication on IBM QRadar

In TLS over TCP communication between IBM Disconnected Log Collector and QRadar, certificate-based communication is used to establish a *chain of trust* in which hardware and software is validated from the end entity to the root certificate.

Before you begin

You must have a root certificate that was issued by a trusted certificate authority (CA). Typically, you use the same root certificate on the Disconnected Log Collector and QRadar computers. Ensure that the root certificate has a meaningful name, such as `root-ca.cer`.

About this task

Every certificate has a validity period (a date range) during which it can be used to establish secure communications. After the validity period ends, the certificate expires and must be replaced.

Procedure

1. Use SSH to log in to the Event Collector, Event Processor, or QRadar Console that will receive events from the Disconnected Log Collector instance.
2. Copy the root certificate to `/etc/pki/ca-trust/source/anchors` and run the following command to update the default truststore:

   ```
   update-ca-trust
   ```

3. To configure the server certificate signing request (CSR), create a file with the following information:

   ```
   [ default ]
   # Change the following line to include the FQDN and IP address of the QRadar
   Console or host
   SAN = DNS:<ec.example.com>,IP:<IP_address>
   [ req ]
   default_bits       = 2048          # RSA key size; change to 4096 if required by
   your organization
   encrypt_key        = no            # Protect private key
   default_md         = sha256        # MD to use
   utf8               = yes           # Input is UTF-8
   string_mask        = utf8only      # Emit UTF-8 strings
   prompt             = no              # Prompt for DN
   distinguished_name = server_dn     # DN template
   req_extensions     = server_reqext # Desired extensions
   [ server_dn ]
   organizationName       = <your_organization_name>
   organizationalUnitName = <your_organizational_unit_name>
   commonName             = <common_name> # Should match a listed SAN
   [ server_reqext ]
   keyUsage             = critical,digitalSignature,keyEncipherment
   extendedKeyUsage     = serverAuth,clientAuth
   subjectKeyIdentifier = hash
   subjectAltName       = $ENV::SAN
   ```

4. Save the file as `/tmp/tls-server.conf` or in your preferred location.

5. Generate a server certificate signing request (CSR) and private key pair by using the following command:

   ```
   openssl req -new -config /tmp/tls-server.conf -out /tmp/tls-server.csr -keyout /tmp/tls-
   server.key
   ```

   A server CSR file is saved as `/tmp/tls-server.csr` and a private key file is saved as `/tmp/tls-server.key`.
6. Submit the CSR to your internal or commercial certificate authority for signing, according to their instructions. The procedure might involve opening the CSR file and copying a block of encoded text that is contained between BEGIN and END markers.
7. Copy the returned client certificate to `/tmp` or your preferred location.
8. The server certificate must be in PKCS#12 format. If the certificate you received is in another format, such as Distinguished Encoding Rules (DER), convert it to PKCS#12 format.

   A certificate's file extension does not necessarily indicate the encoding method used. For example, a certificate with a .cer extension might have Base-64 or DER encoding. Typically, you choose the encoding method during the certificate request procedure. Search the internet for the latest and most complete information about OpenSSL commands to convert certificates from one format to another. For example, use the following commands to convert from DER to PEM to PKCS#12:

   ```
   openssl x509 -inform der -in /tmp/<signed_certificate_file_name>.der -out /tmp/<pem_file_name>.pem
   openssl pkcs12 -export -out /tmp/<pfx_file_name>.pfx -inkey /tmp/tls-server.key -in /tmp/<pem_file_name>.pem
   ```

   Choose a secure password when prompted.
9. Copy the server certificate to `/opt/qradar/conf/key_stores`. If the `/key_stores` folder doesn't exist, create it.

Setting up TLS over TCP communication with IBM QRadar

Transport Layer Security over the Transmission Control Protocol (TLS over TCP) provides encrypted and authenticated communication between IBM Disconnected Log Collector and QRadar.

Before you begin

TLS over TCP requires certificate-based authentication between IBM Disconnected Log Collector and QRadar. For more information, see "Setting up certificate-based authentication on IBM Disconnected Log Collector" on page 5 and "Setting up certificate-based authentication on IBM QRadar" on page 6.

Procedure

1. Log in to the Disconnected Log Collector computer or VM as the root user.
2. Open the `/opt/ibm/si/services/dlc/conf/config.json` file in a text editor.
3. In the **destination.type** parameter, enter TLS (this should already be set by the certificate-based authentication procedure):

   ```
   'destination.type': 'TLS'
   ```

4. In the **destination.ip** parameter, enter the IP address for the Event Collector, Event Processor, or QRadar Console that will receive events from the Disconnected Log Collector instance. For example:

   ```
   'destination.ip':'192.168.0.2'
   ```

5. Save and close the `config.json` file.
6. Restart Disconnected Log Collector by using the following command:

   ```
   systemctl restart dlc
   ```

What to do next

Now you're ready to add IBM Disconnected Log Collector as a log source in QRadar. For more information, see "Adding IBM Disconnected Log Collector as a log source in IBM QRadar" on page 8.

Adding IBM Disconnected Log Collector as a log source in IBM QRadar

To collect events from Disconnected Log Collector, you must install the Disconnected Log Collector protocol and complete configuration steps on your QRadar system.

Procedure

1. If your QRadar Console isn't configured to receive automatic updates, download the Disconnected Log Collector protocol from IBM Fix Central (ibm.com/support/fixcentral/). Using SSH, log in to the QRadar Console as the root user, copy the protocol RPM file to `/tmp` or your preferred location, navigate to the folder, and type the following command:

   ```
   yum -y install <rpm_filename>
   ```

2. Log in to the QRadar user interface as an administrator.
3. In IBM QRadar V7.3.1 or later, click the navigation menu (☰), and then click **Admin**.
4. Click **Advanced** > **Deploy Full Configuration**.

   QRadar continues to collect events when you deploy the full configuration.
5. In the **Data Sources** section, click **Log Sources**.
6. Click **Add**, and then configure the following protocol-specific parameters for Disconnected Log Collector:

Option	Description
Log Source Name	Enter a name for the Disconnected Log Collector log source (for example, `DLC TLS Protocol`).
Log Source Type	Select **Universal DSM**.
Protocol Configuration	Select **IBM QRadar DLC Protocol**.
Log Source Identifier	Enter a unique identifier string (for example, the IP address of a computer on which Disconnected Log Collector is installed).
Protocol	Select the communication protocol that is used to get events from Disconnected Log Collector. Choose **TLS** (default) or **UDP**. The setting must match the Disconnected Log Collector protocol setting.
Listen Port	Enter the QRadar server port to which Disconnected Log Collector sends events. The default port is 32500. For information about how to change the destination port, see "Changing the IBM QRadar server destination port" on page 3.
Authentication by Common Name	The Disconnected Log Collector authentication method. If selected, authentication is by the Common Name (UUID) of the client certificate, which is passed by Disconnected Log Collector. If not selected, authentication is by the alias name of the certificate issuer, which is passed by Disconnected Log Collector.
CN/Alias Whitelist	If authentication is by Common Name, enter the UUID of the Disconnected Log Collector instance as the Common Name. If there's more than one instance, enter a comma-separated list of the UUIDs.

Option	Description
	If authentication is by the alias name of the certificate issuer, enter the alias name of the Disconnected Log Collector certificate issuer. **Tip:** To see a list of aliases that are in the truststore, run the following command: `keytool -list -v -keystore /etc/pki/ca-trust/extracted/java/cacerts | grep Alias`
Key Store File Name	The file name of the server personal exchange format (PFX) certificate, which is located in `/opt/qradar/conf/key_stores` on the Event Collector, Event Processor, or QRadar Console that will receive events from the Disconnected Log Collector instance.
Key Store Password	The password for the server PFX certificate.
Check Revocation	Select the check box to check if the certificate has been revoked.
Trust Store File Path	The file path of the QRadar server truststore (by default, `/etc/pki/ca-trust/extracted/java/cacerts`).
Trust Store Password	The password for the server trust store (by default, *changeit*).
Target Event Collector	The Event Collector, Event Processor, or QRadar Console that will receive events from the Disconnected Log Collector instance.

7. Click **Save**.
8. In the **Admin** settings, click **Deploy Changes**.

Forwarded events

The **IBM QRadar DLC Protocol** exists to bring forwarded events from one or more IBM Disconnected Log Collector instances into the IBM QRadar system.

Forwarded events from log source types that are autodetectable are autodetected as if the events were sent directly to QRadar, except the protocol type is **Forwarded** regardless which protocol the Disconnected Log Collector instance used to collect them. If events are sent by using Transport Layer Security over the Transmission Control Protocol (TLS over TCP), then the Log Source Identifier of the autodetected log source includes the UUID of the forwarding Disconnected Log Collector instance (for example, *192.0.2.0277f291f-dca9-4c59-978a-9d6deb0223b0*). This is to ensure proper separation of event data.

Forwarded events from log source types that are not autodetectable by default require additional action. You can create log sources for these events, singularly or in bulk, by using the QRadar **Log Sources** window, the Log Source Management app, or the Log Sources REST API. The only special consideration for events that are forwarded by a Disconnected Log Collector instance is that the log sources' **Protocol Configuration** parameter must be set to **Forwarded**. Also, if the events are sent by using TLS over TCP, then the Log Source Identifier must include the UUID of the forwarding Disconnected Log Collector instance.

Alternatively, in QRadar V7.3.2, you can configure **Log Source Autodetection** for log source types that are not autodetectable by default. You can configure autodetection for any log source type (custom or IBM provided) by using the DSM Editor **Configuration** tab.

To learn more about adding log sources singularly, in bulk, or by using **Log Source Autodetection**, see the *DSM Configuration Guide*.

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