CORRELOG AGENT FOR IBM ZOS

The CorreLog Agent for IBM z/OS DSM for IBM Security QRadar can collect event logs from your IBM z/OS servers.

The following table identifies the specifications for the CorreLog Agent for IBM z/OSDSM:

Table 5-1 CorreLog Agent for IBM z/OS DSM specifications

Specification	Value
Manufacturer	CorreLog
DSM	CorreLog Agent for IBM z/OS
RPM file name	DSM-CorreLogzOSAgent_*qradar-version_build-number*.noarch.rpm
Supported versions	7.1 7.2
Protocol	Syslog LEEF
QRadar recorded events	All events
Auto discovered	Yes
Includes identity	No
For more information	*Correlog web site* (https://correlog.com/solutions-and-services/sas-correlog-mainframe.html)

CorreLog Agent for IBM z/OS DSM integration process

To integrate CorreLog Agent for IBM z/OS DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent CorreLog Agent for IBM z/OS RPM on your QRadar Console.
2. For each CorreLog Agent instance, configure your CorreLog Agent system to enable communication with QRadar.
3. If QRadar does not automatically discover the DSM, for each CorreLog Agent system you want to integrate, create a log source on the QRadar Console.

Related tasks

Manually installing a DSM

Configuring your CorreLog Agent system for communication with QRadar

Configuring a CorreLog Agent for IBM z/OS log source in QRadar

Configuring your CorreLog Agent system for communication with QRadar

For the procedure to configure your Correlog Agent system for communication with QRadar, see the CZA - CorreLog Agent for z/OS manual that you received from CorreLog with your Agent for z/OS software distribution.

Use the following sections of the guide:

- General considerations in **Section 1: Introduction**.
- Procedure in **Section 2: Installation**.
- Procedure in the **Section 3: Configuration**.

  Ensure that you complete the **Tailoring the Installation for a Proprietary Syslog Extension/IBM Security QRadar** instructions.

  When you start the CorreLog agent, if QRadar does not collect z/OS events, see the **Troubleshooting** topic in Section 3 or contact Correlog Customer support.
- If you want to customize the optional CorreLog Agent parameter file, review QRadar normalized event attributes in **Appendix G: Fields**.

Configuring a CorreLog Agent for IBM z/OS log source in QRadar

To collect CorreLog Agent for IBM zOS events, configure a log source in QRadar.

Procedure

Step 1 Log in to QRadar.

Step 2 Click the **Admin** tab.

Step 3 In the navigation menu, click **Data Sources**.

Step 4 Click the **Log Sources** icon.

Step 5 Click **Add**.

Step 6 From the **Log Source Type** list, select **CorreLog Agent for IBM zOS**.

Step 7 From the **Protocol Configuration** list, select **Syslog**.

Step 8 Configure the remaining parameters.

Step 9 Click **Save**.

Step 10 On the **Admin** tab, click **Deploy Changes**.