Miradore connector for Microsoft WSUS

Version information

Connector version: 2.3.2

Released in Miradore version: 5.1.0

Released: 6/2019

Description

Connector for importing security update information from Microsoft WSUS or SCCM to Miradore.

Supported target systems

Microsoft WSUS 3.0

Software prerequisites

Minimum operation system version: Windows 7 or Windows Server 2008 R2

.NET Framework 4.7.2 or later

Connector host computer

If current WSUS instance uses SQL Server as data storage, connector may be installed on any computer which can connect to both Miradore server and WSUS database server.

If WSUS uses Windows internal database, connector must be installed to WSUS server.

If SCCM is used as datasource, connector can be installed on any computer which can connect to SCCM database.

Configuration changes made by the connector

- Changes made by the installer:
  - Files
    - Creates a program folder (user configurable) and adds files
      - C:\Program Files\Miradore\Connectors\<MiradoreInstance>\WSUS
    - Creates a log folder (user configurable)
      - C:\Program Files\Miradore\Connectors\<MiradoreInstance>WSUS\Logs
  - Registry
    - Connector specific key
      - HKLM\Software\Miradore\Server\Connectors\WSUS
  - Scheduled tasks
    - Adds a scheduled task to run the connector (user configurable)
- Changes made by the program itself
  - Files
    - Creates a log file into the log directory
  - Registry
    - Creates value(s) under the connector specific registry key

Configuration

- Common configuration
  - Miradore server, instance, port and SSL information is entered when installing the connector.
  - These values are saved to the wsus_connector.ini file in the installation directory.
- Connector specific configuration
  - Following connector specific configurations are entered when installing the connector:
    - Data Source (WSUS / SCCM)
    - WSUS computer group / SCCM collection
    - Scanned items (updates and/or computers)
    - Include replica downstream servers
    - Database connection settings
  - If multiple WSUS computer groups or SCCM collections must be configured, this must be done manually to wsus_connector.ini file as described in the connector documentation. Connector can be configured to send data to multiple Miradore instances.

Network connections

- Between connector and Miradore server
  - HTTP(S) connection (port depends on Miradore server configuration, default is 80/443).
- Between connector and WSUS database server

        - TCP connection to database or
        - Named pipe connection to Windows internal database (if WSUS instance uses it as data storage)
    - Between connector and SCCM database (if SCCM is used as data source)
        - TCP connection to database

Authentication

- Between connector and Miradore server
    - Standard Miradore connector authentication (must be authorized from the Miradore UI).
- Between connector and WSUS or SCCM database server
    - Integrated Security (user account which run connector must have read access to database) or
    - SQL Server authentication

Scheduling

- Method
    - By default scheduled as a Windows scheduled task.
- Interval
    - By default once a day.

Principle of operation

- Connect to WSUS/SCCM database
- Read security update information from the database (if updates are configured to be reported)
- Process each WSUS computer group or SCCM collection
    - Connect to Miradore server and check if it is authorized to run
        - Terminate if not authorized
        - Send start event to Miradore server if allowed to run
    - Get list of computers in current group and which has reported since last run
    - Process each computer
        - Get list of computer's security update statuses
        - Write data to output file
    - Send data to Miradore
    - Send stop event to Miradore server

Data transferred to Miradore

- Connector uses public WSUS database views or SCCM database tables to read the data.
- If connector is configured to read security update information, it sends full report of available security updates on every time connector is run.
- If connector is configured to read computer information, it sends report of computers reported since last run. To make sure that Miradore has correct information about computers, connector sends full report of computers every tenth run time.
- Fields in the report are (WSUS database):
    - PUBLIC_VIEWS.vUpdate:
        - DefaultTitle, SecurityBulletin, KnowledgebaseArticle, UpdateId, CreationDate, MsrcSeverity
    - PUBLIC_VIEWS.vUpdateApproval
        - Action
    - PUBLIC_VIEWS.vComputerTarget
        - ComputerTargetId, Name, LastReportedStatusTime
    - PUBLIC_VIEWS.vUpdateInstallationInfo
        - UpdateID, State

Data transferred from Miradore to the target system

- None.

Debugging

- Set value FileLogSeverity in wsus_connector.ini to Debug or Verbose and check the log file.

Version history

- Miradore 5.1.0 / Connector 2.3.2
    - The connector was recompiled with .NET Framework 4.7.2 to ensure compatibility with TLS 1.2 and 1.3 protocols.
- Miradore 4.0.0 / Connector 2.3.0

Improvement: Microsoft SCCM can be used as data source.

Miradore 3.6.4 / Connector 2.2.1

Bug fix: Connector failed to send large amounts of data to Miradore.

Miradore 3.4.0 / Connector 2.2.0

Unicode support

Miradore 3.2.0 / Connector 2.0.1

Proxy support

Changed to use HTTP POST with multipart/form-data

Miradore 2.9.1 / Connector 2.0.0

Support for multiple Miradore instances