



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: DBS-H

Website: www.dbs-h.com

Name of Product: CR8

Version: 2.0.7.60

Date: 29 May 2018 (Revised 25 November 2020)

CR8 OVERVIEW

CR8 is a plug-and-play software solution that enables continuous data integration between relational SQL and BigData/NoSQL database engines.

The CR8 solution provides non-stop data integration by capturing, transforming, routing, and delivering database transactions across heterogeneous database platforms with negligible impact on system performance.

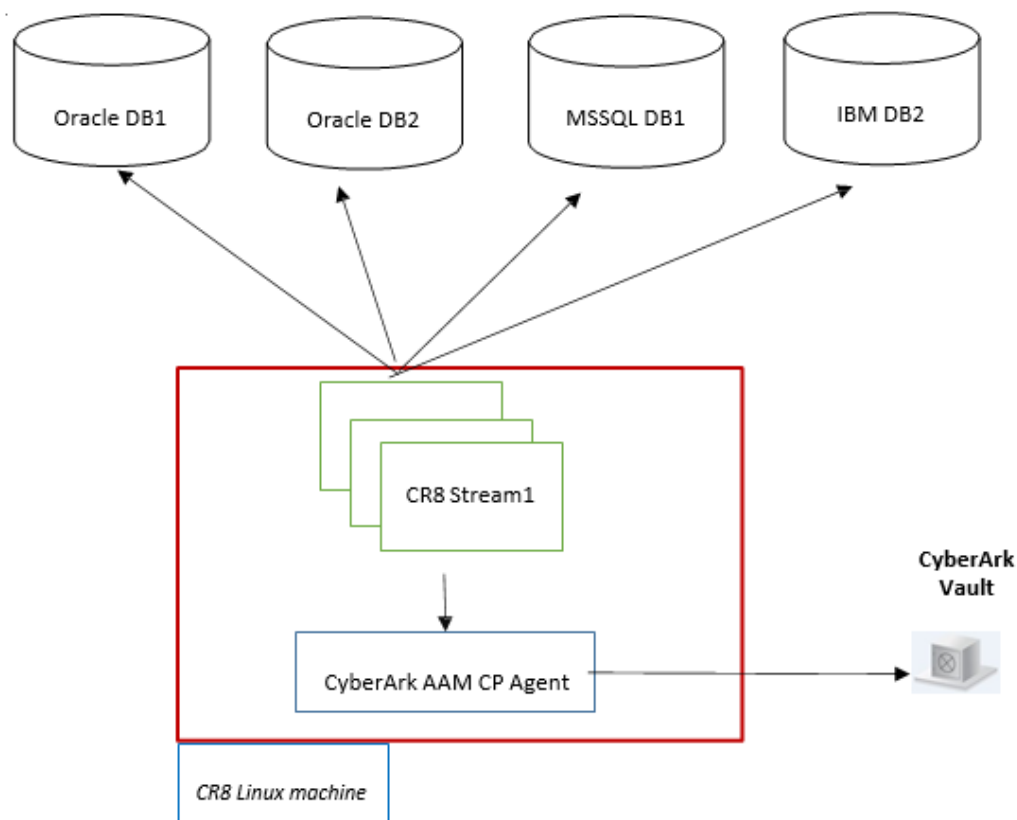
Version: 2.0.7.60

KEY BENEFITS

CR8 enables streaming in of real-time transactions from legacy databases like Oracle/MSSQL/DB2 to Hadoop or NoSQL engines. The solution enables integration of real-time data from existing critical systems into new BigData projects without a need to change existing applications.

CR8 is a Java application that connects to the critical database systems using database username and password. The task of password management is always a security challenge for any enterprise software application. Tight integration between CR8 and CyberArk Secrets Manager allows to meet industry standard requirements and manage database access credentials in the most secure manner.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Deployment:

- CR8 is a Java application deployed in an independent Linux server. CR8 connects to the source Oracle database to capture transactions in real time. Connection is established using native database protocol using database username and password.
- CR8 Stream is an independent Java process that is responsible for capturing changes from a single source database. There many CR8 Streams running in parallel in a typical customer deployment. Multiple CR8 Streams can run inside the same Linux machine or on multiple Linux servers.
- CR8 Stream integrates with a CyberArk Secrets Manager on the “End Point” location. The Secrets Manager Agent is installed and runs inside the CR8 Linux server. CR8 Stream connects to the Secrets Manager using CyberArk Java SDK to retrieve password of the specific database user. Every CR8 Stream performs communication with Secrets Manager independently. If there are multiple CR8 Linux servers available then Secrets Manager is installed on each server to serve local CR8 Streams.

CREDENTIAL RETRIEVAL

CR8 constantly communicates with the source database. Communication is established every 1- 2 seconds to capture new transactions from the source database. At the beginning of every cycle, CR8 communicates with the Secrets Manager to retrieve database login credentials.

CR8 runs on Linux and requires the Secrets Manager Agent to be installed on the same Linux machine.

REQUIREMENTS

CR8 requires a Linux server.

SECRETS MANAGER INSTALLATION

Refer to the [“Credential Provider and ASCP Implementation Guide”](#) for CyberArk Agent based installation and configuration.

DBS-H: Secrets Manager installation and configuration is the customer’s responsibility and is not done by CR8 team.

SECRETS MANAGER CONFIGURATION

The following sections provide details on CR8 configuration with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.

The screenshot shows a 'Add Application' dialog box with the following fields and options:

- Name:** dbsh_cr8
- Description:** (empty text box)
- Business owner:**
 - First Name:** (empty text box)
 - Last Name:** (empty text box)
 - Email:** (empty text box)
 - Phone:** (empty text box)
- Location:** (dropdown menu showing '\')
- Access Permitted:** (unchecked checkbox) with 'From:' and 'To:' dropdown menus.
- Expiration Date:** (unchecked checkbox) with a date picker.
- Disabled:** (unchecked checkbox)

At the bottom of the dialog are 'Add' and 'Cancel' buttons.

- ☐ Specify the following information:
 - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: dbsh_cr8
 - In the **Description** box, specify a short description of the application that will help you identify it.
 - In the **Business owner** section, specify contact information about the application's business owner.
 - In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.

- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. **Partner should suggest the authentication details to secure the access by the partner's application.**
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.

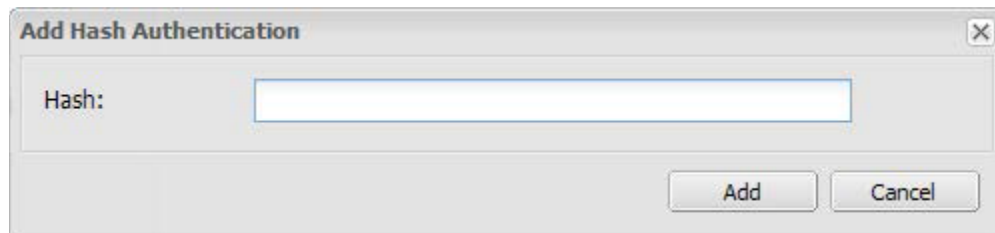
The screenshot shows the 'Add Operating System User Authentication' dialog box. It has a title bar with a close button. Inside, there is a label 'OS User:' followed by a text input field. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Select **Path**. The Add Path Authentication window appears.

The screenshot shows the 'Add Path Authentication' dialog box. It has a title bar with a close button. Inside, there is a label 'Path:' followed by a text input field. Below the input field, there are two checkboxes: 'Path is folder' and 'Allow internal scripts to request credentials on behalf of this application ID'. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- ☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.
- ☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.
- ☐ Specify a hash:

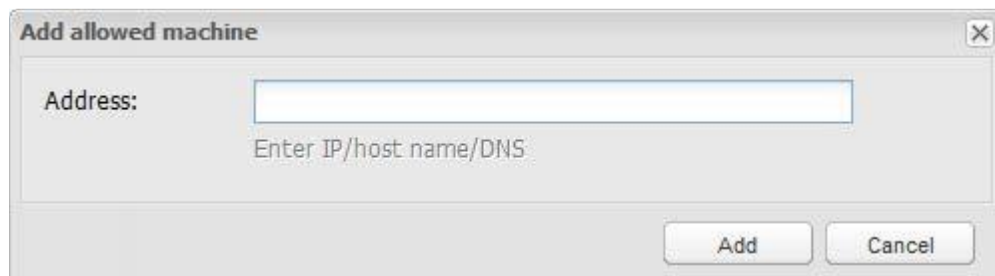
- Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
- In the PVWA, select **Hash**. The Add Hash window appears.



The 'Add Hash Authentication' dialog box has a title bar with a close button. It contains a label 'Hash:' followed by a text input field. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2
Note: The comment must not include a colon or a semicolon.
- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.

- ☐ Specify the application's Allowed Machines. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their passwords.
- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.



The 'Add allowed machine' dialog box has a title bar with a close button. It contains a label 'Address:' followed by a text input field. Below the input field is a placeholder text 'Enter IP/host name/DNS'. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

Make sure the servers allowed include all mid-tier servers or all endpoints where the Secrets Manager Credential Providers were installed.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

- List accounts
- Retrieve accounts
- View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

Add Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☒ View Safe Members

Add

Close

- ☐ Add the application (the APPID) as a Safe Member with the following authorizations:
- Retrieve accounts

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
dbsh_cr8	melkin@dbs-h.com	Michael Elkin

☐ Access
☒ Use accounts
☒ Retrieve accounts
☐ List accounts
☐ Account Management
☐ Safe Management
☐ Monitor
☐ View Audit log
☐ View Safe Members

dbsh_cr8 has been added.

- ☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

CR8 INSTALLATION & INTEGRATION CONFIGURATION

CR8 installation

CR8 product is installed in a form of a Linux rpm package. In order to install the latest version of the CR8 do the following:

1. Log in to the cr8 machine as root OS user

2. Download the latest cr8 rpm package to /tmp directory
3. Install the rpm package by running Linux command : rpm -ivh <cr8 rpm package name>

CR8 product configuration with the CybeArk Secrets Manager

1. In order to retrieve password from a CyberArk password management system, CR8 Stream parameter basicProperties.source.adminSchemaPassword should be populated as follows dbshCyberArk:<full path to the CyberArk configuration file>
2. The CyberArk configuration file includes various parameters that are required for CyberArk for successful authorization.
3. The file should be located under /home/dbsh/cr8/latest_cr8/etc directory and should be based on the existing template file dbshCyberArk_stream.json.template
4. Copy the template file dbshCyberArk_stream.json.template to dbshCyberArk_<stream name>.cfg and fill parameters with missing values
 - appld=
 - objectName=
 - safeName=
 - reason=CR8
 - port=18923
 - timeout=6000
 - folderName=
 - failRequestOnPasswordChange=true

Please consult with CyberArk administrator to fill the above configuration file.

>>Replace this screenshot with your actual integration configuration screenshots:

Partner Application UI:

The screenshot displays a web form for configuring a partner application. It includes input fields for 'Username:' and 'Password:'. Below these is a checkbox labeled 'Use CyberArk Vault to fetch credentials:'. If this checkbox is selected, a second set of input fields appears, including 'Username:', 'Address:', 'Platform (PolicyID):', 'Safe:', 'Folder:' (with 'Root' pre-filled), and 'Object:'.

>>Replace this with your actual configuration options.

Common use cases:

1. Windows domain credentials or other standard credentials
 - a. The user will specify: username, address, platform
 - b. Safe name – optional but recommended for increasing performance
2. Local accounts (windows/Unix)
 - a. The user will specify: username & platform
 - b. Safe name – optional but recommended for increasing performance
 - c. When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned
3. Non-standard credentials (can't be unique with username+address+Platform)
 - a. The user will specify: Safe and object name (folder is usually root by default)

PARTNER CONTACT INFO

Business Contact	Name	Michael Elkin
	Email	melkin@dbb-h.com
	Tel	+972 (54) 689-4212
Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	
	Email	
	Tel	