CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: AppDynamics

Website: www.appdynamics.com

Name of Product: Database Visibility

Version: >= 4.4

Date: December 6, 2017 (Revised October 17, 2020)

APPDYNAMICS DATABASE VISIBILITY OVERVIEW

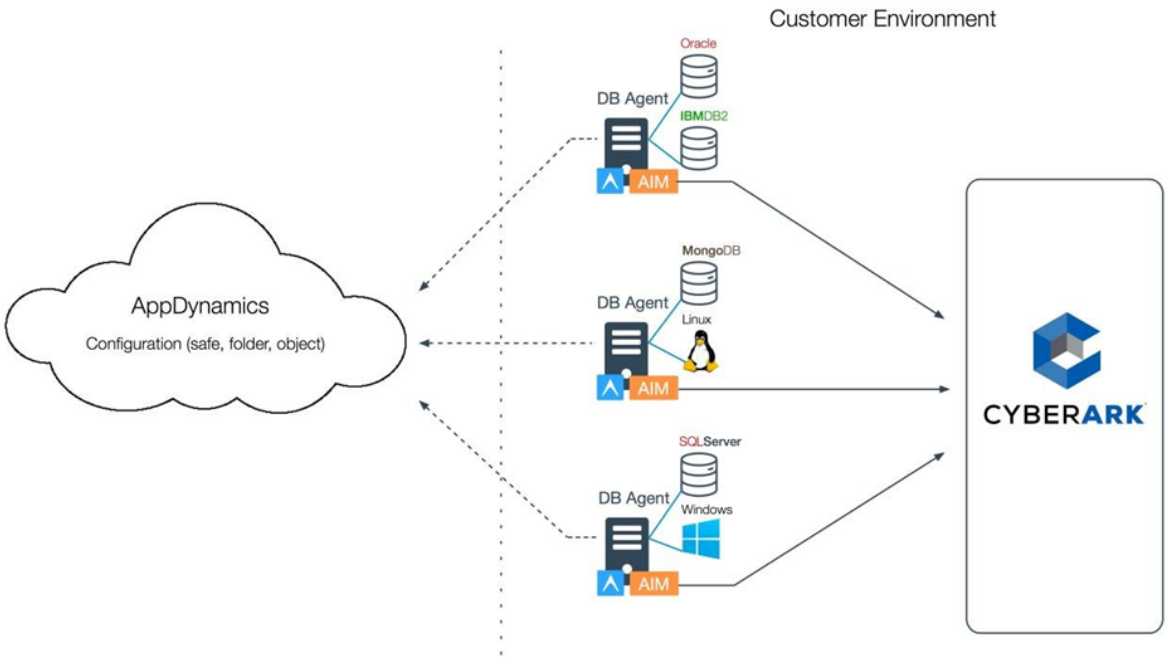
Version: AppDynamics Database Visibility 4.4 , 4.5

KEY BENEFITS

AppDynamics Database Visibility provides insight into database performance by detecting bottlenecks, errors, and more. These metrics allow enterprises to respond quickly to system crashes and optimize their database performance.

Many customers use CyberArk to secure passwords and prevent unauthorized access. Integrating CyberArk with AppDynamics Database Visibility allows these customers to continue using AppDynamics while complying with security regulations.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Secrets Manager is integrated with the AppDynamics Database Visibility agent. Database Visibility agent is a standalone deployment, and it is not part of any tier. It is installed on a particular node or multiple nodes, depending on the customers' requirements.

The Database Visibility agent has configurations containing CyberArk vault information (safe, folder, et al). The agent communicates with the vault and fetches the database credentials (username, password). If the credentials are valid, the agent connects to the database and begins monitoring.

CREDENTIAL RETRIEVAL

In order to access a database collector, the customer must specify the CyberArk application, safe, folder, and object. The customer retrieves credentials once for each valid database configuration.

REQUIREMENTS

Secrets Manager must be installed on the same host as AppDynamics Database Visibility with the application ID specified in the vault.

SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.

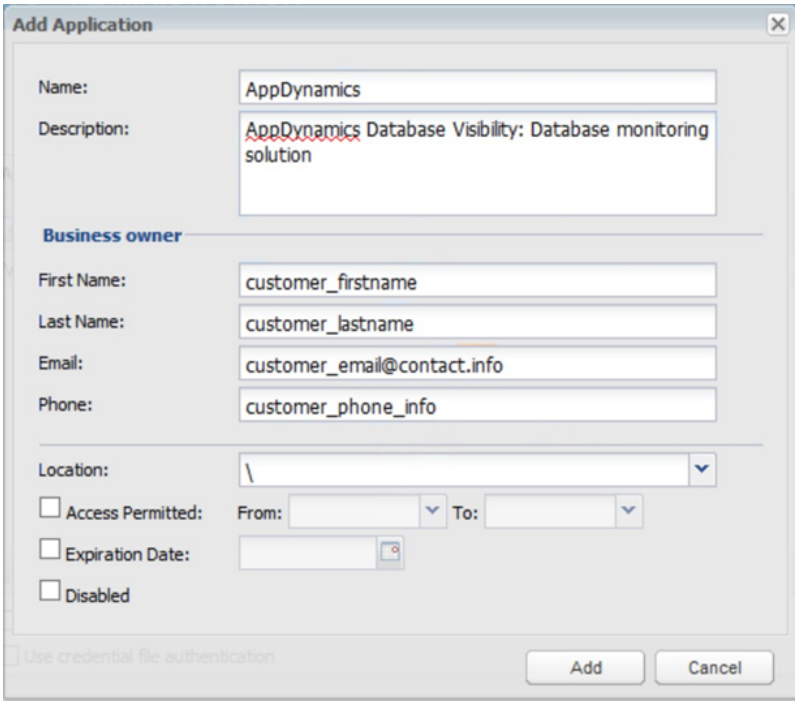
SECRETS MANAGER CONFIGURATION

The following sections provide details on AppDynamics Database Visibility 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:

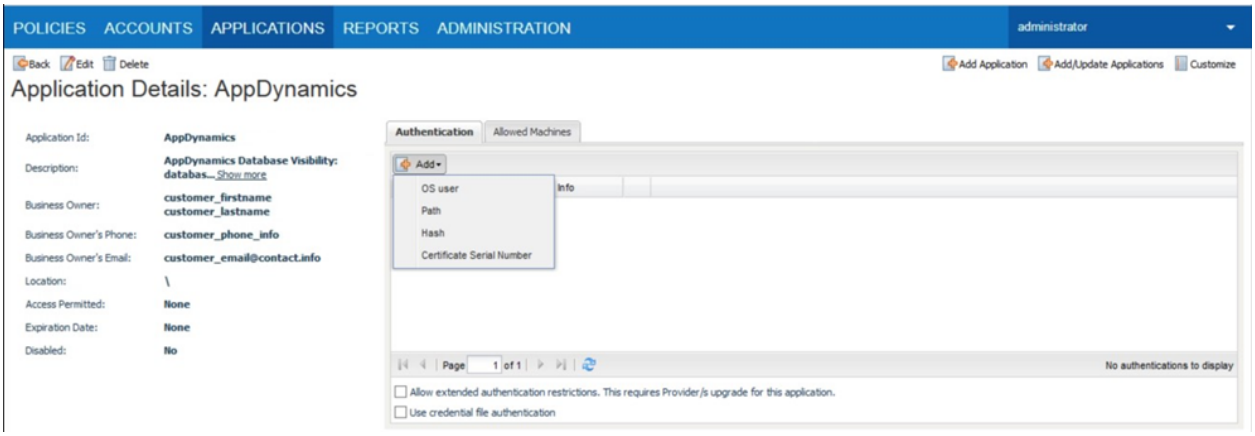
- [ ] Log in as user allowed to manage applications (it requires Manage Users authorization)
- [ ] In the Applications tab, click **Add Application**. The Add Application page appears.



☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: AppDynamics
- 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.



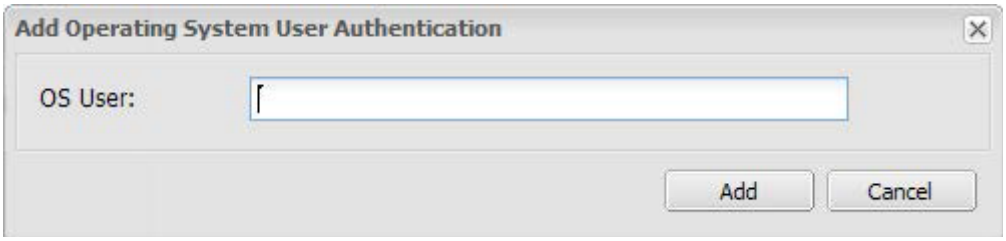
☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.

☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

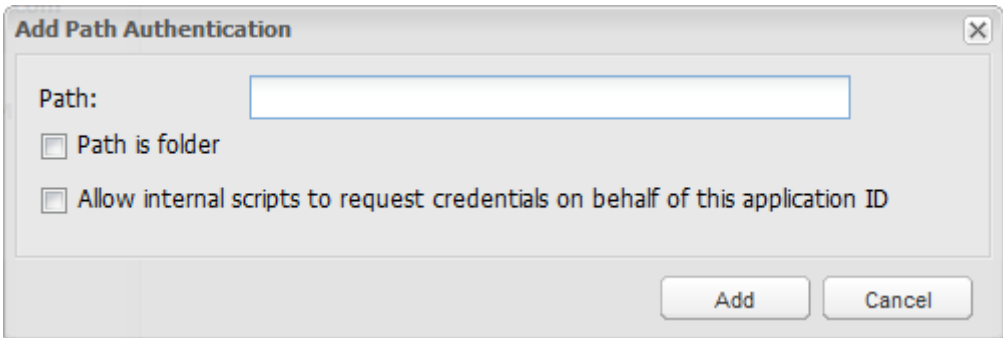
☐ Select the authentication characteristic to specify.

☐ Select **OS user**. The Add Operating System User Authentication window appears.



☐ Specify the name of the OS user who will run the application, then click **Add. T**he OS user is listed in the Authentication tab.

☐ Select **Path**. The Add Path Authentication window appears.



☐ 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:

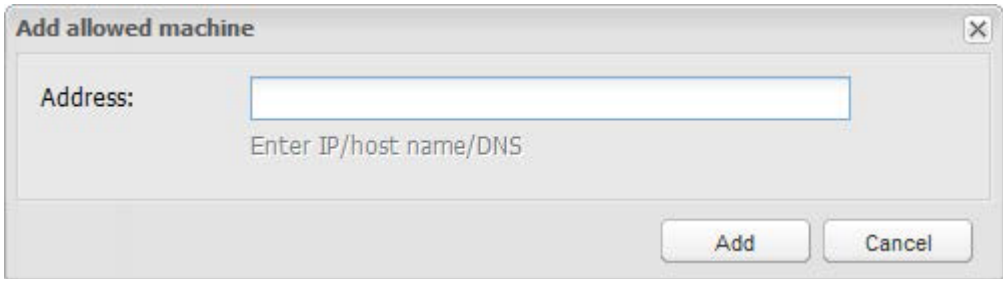
```
java -jar /Users/kbalasubramanyam/cyber-ark/ JavaAIMGetAppInfo.jar GetHash -
AppExecutablesPattern="/Users/kbalasubramanyam/db-agent.jar" -
OnlyExecutablesWithAIMAnnotation=no
```

- Copy the hash value that is returned by the utility.
- In the PVWA, select **Hash**. The Add Hash window appears.

- 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.



- 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.**

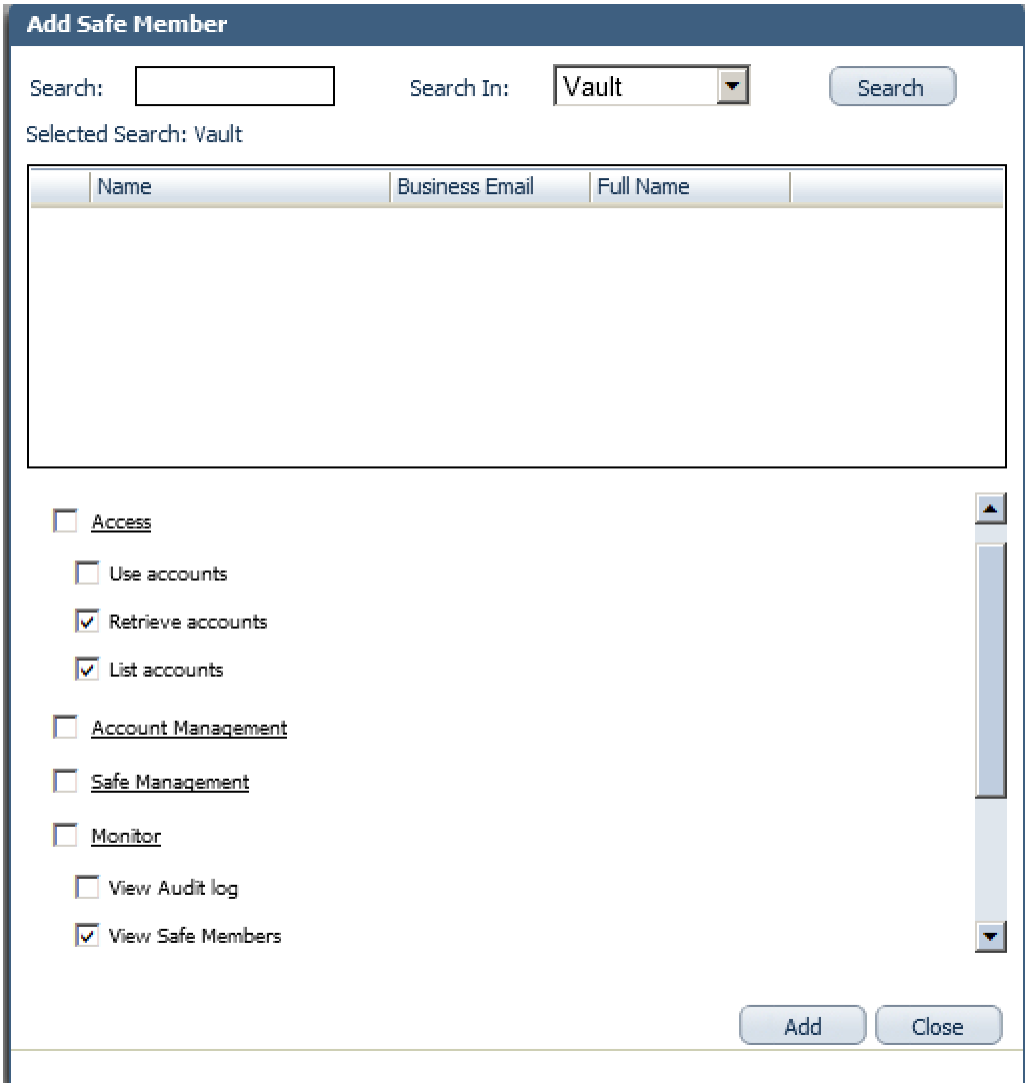
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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:

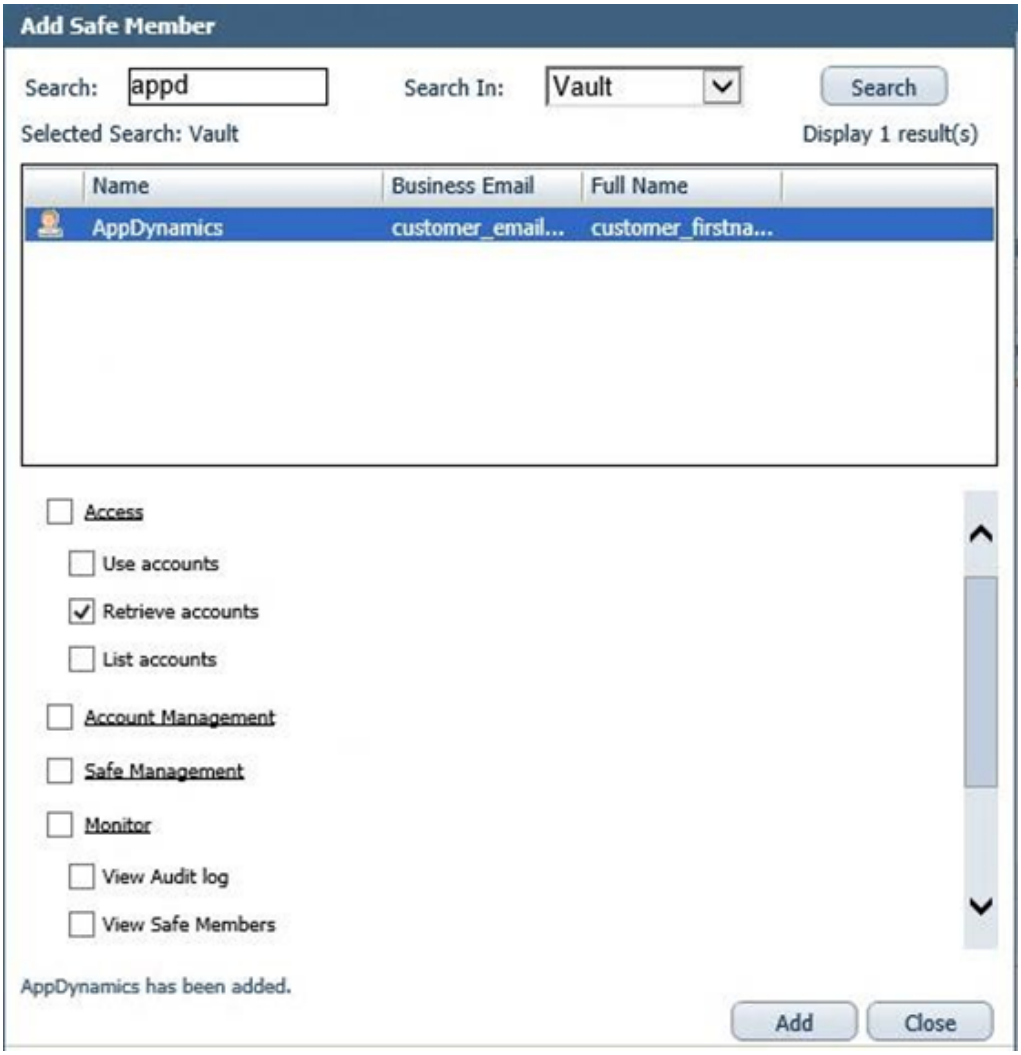
- List accounts
- Retrieve accounts
- View Safe Members

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 the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts



- ☐ 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.

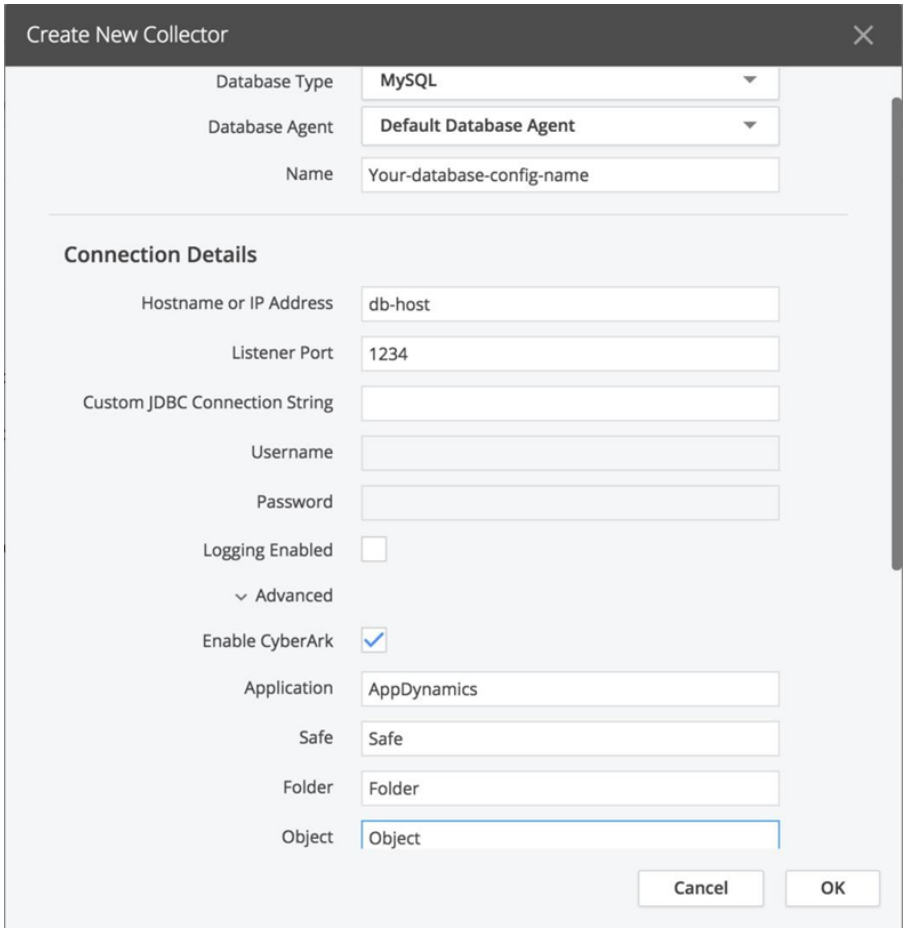
For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

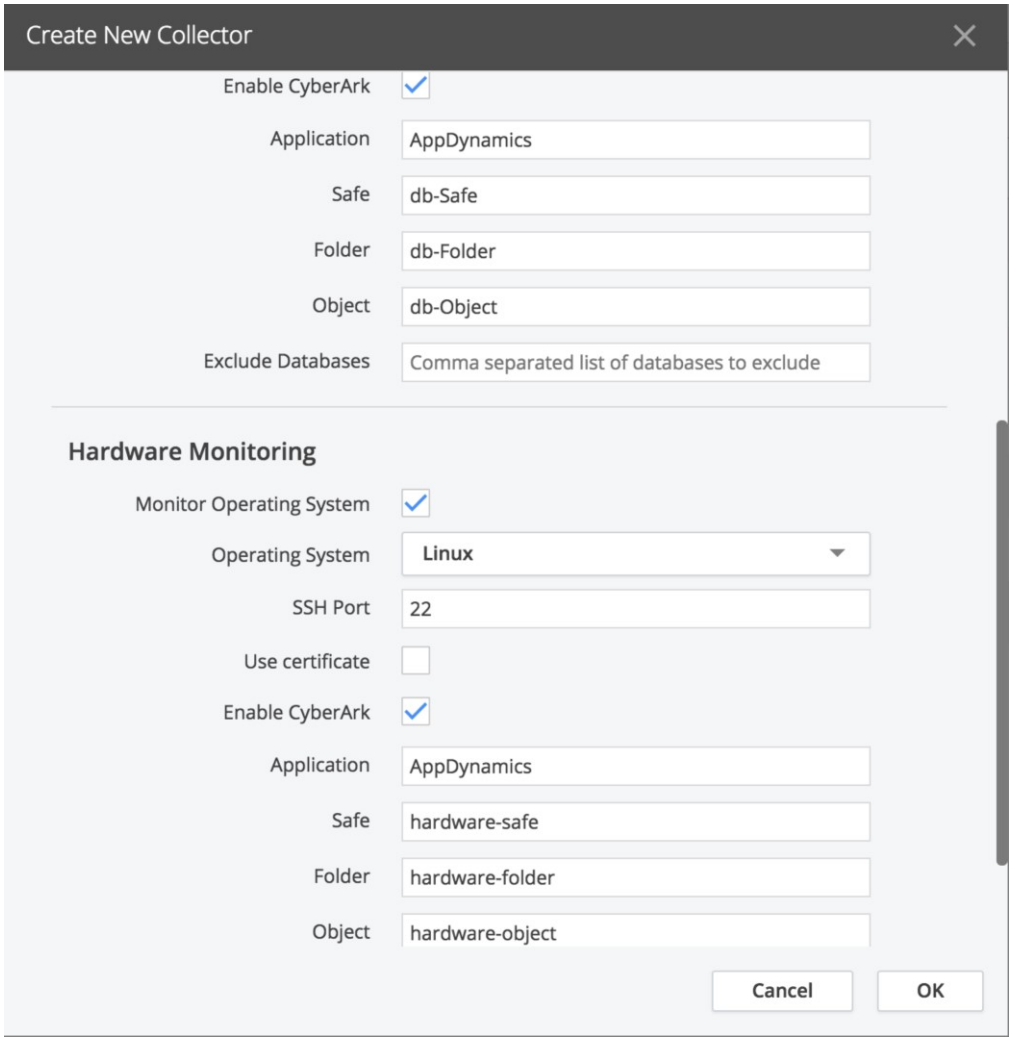
APPDYNAMICS DATABASE VISIBILITY INSTALLATION & INTEGRATION CONFIGURATION

Refer to AppDynamics documentation for AppDynamics Database Visibility installation.

To configure AppDynamics Database Visibility:

1. In the AppDynamics Controller UI, the customer creates database configurations (collectors). If they are using CyberArk, the customer must enable CyberArk (by clicking CyberArk in the dialog box) and provide the vault details (safe, folder, object).
2. The customer deploys the AppDynamics Database Visibility agent on a host along with the Secrets Manager local provider.
3. The agent uses the configuration provided in the AppDynamics Controller to communicate with the CyberArk vault through the Secrets Manager local provider.
4. Once the agent receives all the credentials from the vault, it begins monitoring the customer's databases.





Common use cases:

1. Database platforms
    a. The user will specify: safe, folder, and object.
    b. Application – optional. Useful if customers are running multiple database agents on different hosts with Secrets Manager installed.

2. Hardware platforms
    a. The user will specify: safe, folder, and object.
    b. Application – optional. Useful if customers are running multiple database agents on different hosts with Secrets Manager installed.

PARTNER CONTACT INFO

Business Contact	Name	Ian McGuinness
	Email	imcguinness@appdynamics.com
	Tel	
Technical Contact	Name	Rajneesh Kumar
	Email	rajneesh.kumar@appdynamics.com
	Tel	
Support Contact	Name	Tandav Dutta
	Email	tdutta@appdynamics.com
	Tel	