Informatica

Informatica® Dynamic Data Masking
9.9.1

Transparent Archive Guide

Informatica Dynamic Data Masking Transparent Archive Guide
9.9.1
June 2019

Revision: 1
Publication Date: 2021-06-03

Table of Contents

Preface

The *Transparent Archive Guide* contains information to help administrators implement Transparent Archive for Informatica Data Archive Data Vault and Dynamic Data Masking. This guide assumes that you have knowledge of Data Archive and Data Vault.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

Informatica maintains documentation for many products on the Informatica Knowledge Base in addition to the Documentation Portal. If you cannot find documentation for your product or product version on the Documentation Portal, search the Knowledge Base at https://search.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

Introduction to Transparent Archive

This chapter includes the following topic:

Transparent Archive Overview

You can use Dynamic Data Masking Transparent Archive to seamlessly access the Data Vault and a production database.

Dynamic Data Masking handles the request and acts as a database link between the production database and the Data Vault. Dynamic Data Masking redirects the SQL statement to the Data Vault and receives the result set from the Data Vault. Dynamic Data Masking then constructs the correct production database protocol response from the result set and returns the production database protocol response to the client.

CHAPTER 2

Transparent Archive Configuration

This chapter includes the following topics:

Transparent Archive Configuration Overview

Configure Transparent Archive to seamlessly access the Data Vault and a production database.

Complete the following tasks to configure Transparent Archive:

1. Verify the system requirements.
2. Add the Dynamic Data Masking services in the Management Console.
3. Add the database link listener port to the production database service.
4. Define the Data Vault.
5. Define the production database.
6. Create the connection rules.
7. Create a database link.

Verify the System Requirements

Before you configure Transparent Archive, verify the system requirements.

Verify that the following software is installed to use Transparent Archive:

- Dynamic Data Masking version 9.5.3 or later.
- Informatica Data Archive application working with a Microsoft SQL Server 2005 database or later.

Adding the Dynamic Data Masking Service in the Management Console

Add the Microsoft SQL Server service in the Management Console. If the service exists in the Management Console, add the listener port for the database link.

1. In the Management Console, click the Dynamic Data Masking Server in the tree.
2. Click **Tree** > **Add DDM Services**.

   The **Add DDM Services** window appears.
3. Select the DDM for SQL Server service in the **Add DDM Services** window.
4. Click **OK**.

   The service appears in the Management Console tree.

Adding the Listener Port to the Production Database Service

If the Dynamic Data Masking service database link listener port is not defined, you must add it in the Management Console.

1. In the Management Console, click the production database service in the tree.
2. Click **Tree** > **Edit**.

   The **Edit** window appears.
3. Click **Add Port**.
4. Enter the port number of the database link and click **OK**.

   The **Edit** window closes.

Defining the Data Vault

Define the Data Vault in the Management Console.

1. In the Management Console, click **Tree** > **Add Database**.

   The **Add Database** window appears.
2. Select the FAS database type.
3. Define the following properties for the Data Vault:

   DDM Database Name

   Name for the database that appears in the Management Console tree.

   Server Address

   Server host name or TCP/IP address for the Data Vault.

   Note: Verify that there is no firewall that prohibits the Dynamic Data Masking Server from connecting to the database server and port number.

   Server Port

   TCP/IP listener port for the Data Vault.

   FAS Database Name

   Database name for the Data Vault.

   DBA Username

   User name for the database user account to log in to the Data Vault.

   DBA Password

   Password for database user.
4. Click **Test Connection** to validate the connection to the database.
5. Click **OK**.

   The Data Vault node appears in the Management Console tree.

Defining the Microsoft SQL Server Database

Define the Microsoft SQL Server production database in the Management Console.

1. In the Management Console, click **Tree** > **Add Database**.

   The **Add Database** window appears.
2. Select the SQL Server database type.
3. Define the following properties for the Microsoft SQL Server database:

   DDM Database Name

   Name for the database in the Management Console tree.

   Server Address

   Server host name or TCP/IP address for the Microsoft SQL Server database.

Note: Verify that there is no firewall that prohibits the Dynamic Data Masking Server from connecting to the database server and port number.

Server Port

TCP/IP listener port for the Microsoft SQL Server database that the database link uses.

Optional Parameters

Additional parameters for the Informatica driver for Microsoft SQL Server.

Database Name

Optional name of a Microsoft SQL Server database. Used for manual upgrade of Dynamic Data Masking for Microsoft SQL Server service.

Rule Set

Optional rule set you can define for a specific database in addition to the Default Rule Set. Used for manual upgrade of Dynamic Data Masking for Microsoft SQL Server service.

DDM Port

Dynamic Data Masking listener port. Use DDM Port for a manual upgrade of the Dynamic Data Masking for Microsoft SQL Server service.

Default Rule Set

Rule set that applies to all incoming SQL statement requests. Used for manual upgrade of Dynamic Data Masking for Microsoft SQL Server service.

DBA Username

User name for the database user account to log in to the Microsoft SQL Server database.

DBA Password

Password for the database user.

4. Click **Test Connection** to validate the connection to the database.
5. Click **OK**.

   The Microsoft SQL Server database node appears in the Management Console tree.

Create the Connection Rules

Create a connection rule tree to use Transparent Archive.

The rule tree consists of a rule folder that contains connection rules. The rule folder identifies requests by the incoming listener port and sends the request to the rules in the folder.

The SWITCHTODB rule directs the incoming request to the production database.

You can optionally add a USERULESET rule that applies a security rule set to the request. The security rule set can contain masking and blocking rules to secure sensitive data.

The TRANSPARENTARCHIVE rule uses the Transparent Archive rule action. You can specify the database administrator user name and password for the JDBC connection to the Data Vault.

Note: The rule that uses the Transparent Archive rule action must be the last rule in the connection rule tree. Dynamic Data Masking stops processing the SQL statement after it completes the Transparent Archive rule action.

Creating the Rule Folder

Create a connection rule folder that identifies incoming requests.

1. In the Management Console, select **Tree** > **Connection Rules**.

   The **Rule Editor** window appears.
2. Select **Action** > **Append rule**.

   The **Append Rule** window appears.
3. Enter the port number that you added to the Dynamic Data Masking service for Microsoft SQL Server as the rule name.
4. Select the Incoming DDM Listener Port rule matcher.
5. Define the following parameter for the DDM Listener Port matcher:

   Incoming Port

   The port number that you added to the Dynamic Data Masking service for Microsoft SQL Server.
6. Select the Folder rule action.
7. Select the Stop if Matched processing action.
8. Click **OK**.

   The connection rule folder appears in the rule tree.
9. Select **File** > **Update Rules**.

   The connection rule folder is saved.

Creating the Switch to Database Rule

Create a rule that uses the Switch to Database rule action.

1. In the **Rule Editor**, click the listener port rule folder in the rule tree, and select **Action** > **Append rule**.

   The **Append Rule** window appears.
2. Enter SWITCHDB as the rule name.
3. Select the All Incoming Connections matcher.
4. Select the Switch to Database rule action.
5. Define the following rule action parameter:

   Database

   The name of the production database that you defined in the Management Console.
6. Select the Continue processing action.
7. Click **OK**.

   The connection rule appears in the rule tree.
8. Select **File** > **Update Rules**.

   The connection rule is saved.

Creating the Use Rule Set Rule

Optionally, create a rule that directs the Rule Engine to a security rule set.

1. In the **Rule Editor**, click the listener port rule folder in the rule tree, and select **Action** > **Append rule**.

   The **Append Rule** window appears.
2. Enter USERULESET as the rule name.
3. Select the All Incoming Connections matcher.
4. Select the Use Rule Set rule action.
5. Define the following rule action parameter:

   Rule Set Name

   The name of the rule set that contains the masking rules that you want to apply.
6. Select the Continue processing action.
7. Click **OK**.

   The connection rule appears in the rule tree.
8. Select **File** > **Update Rules**.

   The connection rule is saved.

Creating the Transparent Archive Rule

Create a connection rule that uses the Transparent Archive rule action.

1. In the **Rule Editor**, select **Action** > **Append rule**.

   The **Append Rule** window appears.
2. Enter TRANSPARENTARCHIVE as the rule name.
3. Select the All Incoming Connections matcher.
4. Select the Transparent Archive rule action.
5. Define the following rule action parameters:

   DDM Database Name

   The Dynamic Data Masking database name for the Data Vault that you defined in the Management Console.

   DBA User

   The user name for the Data Vault. This field overrides the database administrator user name that you defined in the Management Console. Dynamic Data Masking uses this field for the connection to the Data Vault.

   DBA Password

   The password for the Data Vault user. This field overrides the database administrator password that you defined in the Management Console. Dynamic Data Masking uses this field for the connection to the Data Vault.
6. Select the Stop if Applied processing action.
7. Click **OK**.

   The connection rule appears in the rule tree.
8. Select **File** > **Update Rules**.

   The connection rule is saved.

Create a Database Link

Create a database link before you configure Transparent Archive.

You must create a database link between the production database and the Dynamic Data Masking service that you configured to connect to the production database.

The database link must point to the Dynamic Data Masking for Microsoft SQL Server service that you configured. The database link uses the port that you defined for the Dynamic Data Masking for Microsoft SQL Server service.

CHAPTER 3

Dynamic Data Masking

This chapter includes the following topics:

Dynamic Data Masking Overview

Dynamic Data Masking is a data security product that operates between an application and a database to prevent unauthorized access to sensitive information. Dynamic Data Masking intercepts requests sent to the database and applies data masking rules to the request to mask the data before it is sent back to the application.

You can use Dynamic Data Masking to mask or prevent access to sensitive data stored in production and non-production databases. You set up the rules to specify the database requests to intercept and the masking actions to apply. Dynamic Data Masking monitors incoming database requests from the application. Dynamic Data Masking applies the data masking rules to the database request before it sends it to the database. The database processes the modified request as normal and returns masked results to Dynamic Data Masking. Dynamic Data Masking then sends the results to the application.

You can use Dynamic Data Masking to mask data for specific types of database requests or you can restrict access to data from certain groups within an organization. For example, you can create a rule to apply a masking function to credit card numbers when the database request comes from a support team member. When the database sends the data back to the application, the support team member sees the masked numbers instead of the real credit card numbers.

Dynamic Data Masking Components

Dynamic Data Masking includes server components to intercept and process database requests and a client component to manage the server.

Dynamic Data Masking has the following components:

Dynamic Data Masking Server

The Dynamic Data Masking Server provides services and resources to intercept database requests and perform data masking tasks.

The Dynamic Data Masking Server includes the following components:

- Dynamic Data Masking services
- Rule Engine

Dynamic Data Masking Service

The Dynamic Data Masking service listens on the listener port to monitor and route incoming database requests.

You can run the following Dynamic Data Masking services:

Service	Description
DDM for Azure	Listens for and routes database requests for a Microsoft Azure SQL database. The service supports the SSL mode of communication.
DDM for DB2	Listens for and routes database requests for an IBM Db2 database. The service supports SSL and non-SSL modes of communication.
DDM for FAS	Listens for and routes database requests for Data Vault. The service supports SSL and non-SSL modes of communication.
DDM for Hive	Listens for and routes database requests for a Hive database. The service supports SSL and non-SSL modes of communication as well as Kerberos Authentication and Kerberos encrypted data.
DDM for Hive HTTP	Listens for and routes database requests for Hive databases using HTTP transport. The service supports SSL and non-SSL modes of communication, and Kerberos Authentication.
DDM for Impala	Listens for and routes database requests for an Impala database. The service supports SSL and non-SSL modes of communication as well as Kerberos Authentication.
DDM for Informix	Listens for and routes database requests in Informix native protocol to Informix databases.
DDM for Informix (DRDA)	Listens for and routes database requests in Distributed Relational Database Architecture protocol to Informix databases.
DDM for JDBC	Listens for database requests for a database that uses JDBC connectivity.
DDM for ODBC	Listens for database requests for a database that uses ODBC connectivity.
DDM for Oracle	Listens for and routes database requests for an Oracle database. The service supports SSL and non-SSL modes of communication.
DDM for PostgreSQL	Listens for and routes database requests for a PostgreSQL database.
DDM for SQL Server	Listens for and routes database requests for a Microsoft SQL Server database. The service supports SSL and non-SSL modes of communication.
DDM for Sybase	Listens for and routes database requests for a Sybase database.
DDM for Teradata	Listens for and routes database requests for a Teradata database.

Rule Engine

The Rule Engine evaluates incoming database requests and applies connection and security rules to determine how to route requests and mask data. The Rule Engine can modify the database request based on the rules defined in the Dynamic Data Masking Server.

The Rule Engine applies the following types of rules:

- Connection rule. Defines the conditions and actions that the Rule Engine applies to determine how to route a database connection request received from an application.
- Security rule. Contains the conditions and actions that define what to do with the database SQL request and how to apply SQL rewrites that manipulate the returned SQL result set.

Server Control

Server Control is a command line program that you use to configure and manage the Dynamic Data Masking Server. Use Server Control to start or stop the Dynamic Data Masking Server and services or to change the port number or password for the Dynamic Data Masking Server.

Management Console

The Management Console is a client application that you use to manage the Dynamic Data Masking Server. You can use the Management Console to create and manage rules and to configure and manage connections to databases.

CHAPTER 4

Dynamic Data Masking Administration

This chapter includes the following topics:

Dynamic Data Masking Administration Overview

As an administrator, you use the Server Control program to manage the Dynamic Data Masking Server and start and stop the Dynamic Data Masking services. You use the Management Console to configure target databases, define listener ports, manage target databases, maintain system logs, and define rules. The administrative tasks that you perform help to ensure that Dynamic Data Masking operates effectively and efficiently.

Note: To prevent loss of data, such as connection rules, security rule sets, and database configurations, perform regular backups of the entire Dynamic Data Masking directory to a location on your network or an external storage location

Management Console

The Management Console is the client component of the Dynamic Data Masking Server.

You can install the Management Console on a remote machine or the local system to manage the Dynamic Data Masking service. Use the Management Console to manage and configure domains and Dynamic Data Masking services, define connection rules for Dynamic Data Masking services, define security rules, and configure target databases.

Navigation

The Management Console is a user interface that you use to create and configure the Dynamic Data Masking domains, databases, services, and rule sets.

The left side of the Management Console contains a hierarchical tree that represents the components of Dynamic Data Masking. The tree contains domain, database, server, service, and rule set nodes. Use the menu and toolbar above the tree to add, edit, remove, cut, copy, paste, and sort items within the tree. You can drag and drop nodes to change the placement of the node within the tree.

The right side of the Management Console contains a view pane with parameters of the node you select in the tree.

Menu

The Management Console Tree menu contains options that you use to edit the nodes within the Management Console tree. The toolbar contains shortcuts to options in the menu. Available menu items change based on the type of node you select in the tree. Items that are not available for the tree node you select are grayed out.

The Management Console Tree menu contains the following options:

Menu Item	Action
Login	Shows the server host, port, and username for the last login.
Exit	Exits the Dynamic Data Masking session.
Add Domain	Creates a domain in the Management Console tree. Add Domain is available when a domain node is selected.
Add Database	Defines the connection properties for an additional database in the Management Console tree. Add Database is available when a domain node is selected.
Add DDM Services	Adds a Dynamic Data Masking service to the Management Console tree. Add DDM Services is available when the server node is selected.
Add Rule Set	Adds a security rule set to the Management Console tree. Add Rule Set is available when a domain node is selected.
Edit	Opens a window to edit domain and rule set names, define service listener ports, and edit connection information for databases and the Dynamic Data Masking Server.
Security Rule Set	Opens a security rule set. Security Rule Set is available when a security rule set is selected.
Connection Rules	Opens a connection rule set. Connection Rules is available when a Dynamic Data Masking service is selected.
Authorization	Opens a window to set and edit permissions for the selected node. Authorization is available when a database, domain, or security rule set node is selected.
Cut	Copies and deletes the selected Management Console tree node. You can cut server, database, domain, and security rule set nodes. You cannot cut service nodes or the root domain node.
Copy	Copies the selected Management Console tree node. You can copy database, domain, and security rule set nodes. You cannot copy service nodes, server nodes, or the root domain node.

Menu Item	Action
Paste	Pastes the cut or copied Management Console tree node. You can paste on domain nodes.
Remove	Removes a node from the Management Console tree. **Note:** You cannot remove the Dynamic Data Masking Server or the Management Console root domain.
Start Service	Starts a Dynamic Data Masking service. The Start Service option is available when a Dynamic Data Masking service is selected.
Stop Service	Stops a Dynamic Data Masking service. The Stop Service option is available when a Dynamic Data Masking service is selected.
Add Logger	Adds a custom logger to the Management Console tree. Add Logger is available when the Loggers node is selected.
Add Appender	Adds an appender to the Management Console tree. Add Appender is available when a logger node is selected.
Support	Creates an encrypted .zip archive of Dynamic Data Masking logs. You can send the log archive to Informatica Global Customer Support to troubleshoot issues with Dynamic Data Masking.
Manage Licenses	Allows you to select a new license file. Use the Manage Licenses option if the Dynamic Data Masking license file has expired. The Manage Licenses option is available when the Dynamic Data Masking Server node is selected.
Sort by Name	Sorts child nodes and nested child nodes in alphabetical order by the name of the node. Sort by Name is available when a node with child nodes is selected.
Sort by Owner	Sorts child nodes and nested child nodes in alphabetical order by the login name of the user that created the nodes. Sort by Owner is available when a node with child nodes is selected.
Sort by Type	Sorts child nodes and nested child nodes in alphabetical order by the type of node. Sort by Type is available when a node with child nodes is selected.

Management Console Tree

The Management Console tree is a navigation tree organized by nodes. When the Management Console is not connected to a Dynamic Data Masking Server, it shows a default domain node. All actions are disabled, except Login, Exit, and About. After successful login to a Dynamic Data Masking Server, the Management Console shows a tree with the Dynamic Data Masking Server node that it is connected to.

The Management Console tree can contain domain, database, server, service, logger, appender, and rule set nodes. Tree nodes are arranged hierarchically.

On the Management Console, the relationship between the Dynamic Data Masking Server and a database is based on the domain organization. The Dynamic Data Masking Server will connect to databases that are in the same domain or a sub domain of the Dynamic Data Masking Server. The Dynamic Data Masking Server will not connect to any database that is outside the domain that contains the Dynamic Data Masking Server.

Logging In to the Management Console

You can access the Dynamic Data Masking components through the Management Console. Log in to the Management Console to manage target databases, configure listener ports, and define rules.

To log in to the Management Console, you need the server address and port number of the server that Dynamic Data Masking operates on and the administrator credentials.

Logging In to the Management Console on Windows

On Windows, open the Management Console through the Start menu.

1. On Windows 7 and earlier, select **Start** > **All Programs** > **Informatica** > **Dynamic Data Masking** > **Management Console**.

   On Windows 10 and later, select **Search the Web and Windows** > **All apps** > **Informatica Dynamic Data Masking** > **Management Console**.

   The **Login** window appears.
2. Verify that the **Server Host** and **Port** display the correct information for the Dynamic Data Masking Server.
3. Enter the Dynamic Data Masking administrator user name and password. If you use LDAP authentication, the user name must be in LDAP format. Click **Connect**.

   A tree is visible in the Management Console after you login successfully.

Logging In to the Management Console on Linux

On Linux, start the Management Console with the `mng` script.

You must have the X Window server installed on the machine that you use to log in to the Management Console.

1. Open a terminal and navigate to the Dynamic Data Masking installation directory.

   For example, you might enter the following command:

   ```
   cd /home/Informatica/DDM
   ```
2. Run the following command to start the Management Console:

   ```
   ./mng
   ```

   The **Login** window appears.
3. Verify that the **Server Host** and **Port** display the correct information for the Dynamic Data Masking Server.
4. Enter the Dynamic Data Masking administrator user name and password. If you use LDAP authentication, the user name must be in LDAP format. Click **Connect**.

   A tree is visible in the Management Console after you log in.

Database Management

A database node contains references to databases. The Dynamic Data Masking Server controls access to the databases that the database nodes reference.

A database node can reference an Oracle, Microsoft SQL Server, Db2, Informix, Sybase, Data Vault, Hive, or Teradata database. The Management Console tree can contain an unlimited number of database nodes. You

can create database nodes under domain nodes. Database nodes do not have child nodes. You can set user permissions on database nodes.

Dynamic Data Masking Server Management

A server node contains a reference to the Dynamic Data Masking Server. By default, the server node is located under the root domain after a new installation of the Dynamic Data Masking Server.

The Management Console contains one server node. Each Dynamic Data Masking instance associates with one Dynamic Data Masking Server. You connect to a server when you log into the Management Console. The Dynamic Data Masking Server manages databases located under a parent domain or all sub domains of the server node in the tree.

The server node has a domain node parent. The server node can have Dynamic Data Masking service child nodes. You can edit and move the server node.

Note: You cannot add or remove the Dynamic Data Masking Server node with the Add or Remove options in the Management Console menu.

Dynamic Data Masking Service Management

The Dynamic Data Masking service routes SQL queries to Oracle, Microsoft SQL Server, Db2, Informix, Sybase, Data Vault, Hive, and Teradata databases.

The Dynamic Data Masking Server can contain single service nodes for each database. Create service nodes under the server node. Service nodes cannot have child nodes. You can add, edit, and remove service nodes.

Each Dynamic Data Masking service routes requests to a specific type of database. For example, the Dynamic Data Masking for Oracle service routes requests to Oracle databases and the Dynamic Data Masking for DB2 service routes requests to Db2 databases.

Dynamic Data Masking Listener Ports

The Dynamic Data Masking service controls connections between the client and the database through the listener port.

You must configure the database listener port to forward connections to the Dynamic Data Masking listener port. How you configure the listener ports depends on whether the Dynamic Data Masking service runs on the database server or on a standalone server. You can define the listener port that the Dynamic Data Masking service uses through the Services Editor in the Management Console.

If the Dynamic Data Masking service runs on a standalone server, you must route application connection requests to the Dynamic Data Masking listener port.

Defining a Dynamic Data Masking Listener Port

Before you can define a listener port, you must run the netstat system utility to verify port availability.

1. In the Management Console, right-click on a Dynamic Data Masking service and select **Edit**.

   The Service Editor appears.

2. Click **Add Port**.
3. Enter the listener port for the Dynamic Data Masking service.
4. Click **OK**.

Deleting a Dynamic Data Masking Listener Port

If the Dynamic Data Masking service no longer uses a listener port, delete the listener port with the Service Editor.

1. In the Management Console, right-click the Dynamic Data Masking service and select **Edit.**

   The Service Editor appears.
2. Select the port to delete.
3. Click **Remove port**.
4. Click **OK**.

Domain Management

A domain is a virtual node in the Management Console tree that you use to group other nodes. The Management Console contains a default root domain. You can use domains to create a visual representation of the structure of the databases within an organization.

You can create an unlimited number of domains in the Management Console tree. A domain can contain other domains, databases, and server child nodes. You can set user permissions on domain nodes.

You can add, edit, cut, copy, paste, and remove a domain. You cannot remove the root domain. Drag a domain up or down in the Management Console tree to change the position of the domain within the tree.

Security Rule Set

A security rule set is a tree node that contains references to one or more security rules. To secure data, you must create security rule sets with masking, rewrite, and blocking actions.

You can add a security rule set to a domain node in the Management Console tree.

The Management Console tree can contain an unlimited number of rule set nodes. Rule sets do not have child nodes. You can add, edit, move, and remove rule set nodes. You can set user permissions on security rule set nodes.

Connection Management Overview

Use the **Add Database** window to add a database to the Management Console tree. Select a database type and define database parameters. Test the database connection to verify that the Dynamic Data Masking service can access the database.

Data Vault Connection Management

To add an Informatica Data Vault connection node to the Management Console tree, select the FAS database type.

You can enable SSL communication between the Data Vault and the Dynamic Data Masking Server. For more information about enabling SSL communication, see the "Security" chapter. Communication is encrypted between the Dynamic Data Masking FAS service and the Data Vault, and between the Dynamic Data Masking FAS service and the Data Vault client. For information on how to enable SSL in the Data Vault, see the *Data Vault Administrator Guide*. To use SSL communication, you must have Data Archive version 6.4.3 or later installed.

Click **Test Connection** to verify that the Dynamic Data Masking service can access the database.

Data Vault Connection Parameters

Define the following connection parameters for a Data Vault connection:

DDM Database Name

Name for the database node that appears in the Management Console tree.

Server Address

Server host name or TCP/IP address for the Data Vault.

Note: Verify that there is no firewall that prohibits the Dynamic Data Masking Server from connecting to the Data Vault Server and port number.

Server Port

TCP/IP listener port for the Data Vault.

FAS Database Name

Database name for the Data Vault.

Keystore

Select **Custom** if you have configured a custom keystore. Select **Default** if you want to use the default keystore preconfigured for use with Dynamic Data Masking.

DBA Username

User name for the Data Vault user account to log in to the Data Vault. The Data Vault user must have the SELECT access privilege for all the tables to which the client user has the SELECT access privilege. This parameter is valid for the default keystore.

DBA Password

Password for the Data Vault user. This parameter is valid for the default keystore.

Key Store Name

Name of the custom keystore, defined in the `ddm.security` file. This parameter is valid for custom keystores.

Alias

Alias name for the custom keystore. For CyberArk accounts, the alias name was defined when the CyberArk account was created. This parameter is valid for custom keystores.

SSL

Select to enable SSL communication between the database and the Dynamic Data Masking Server. For more information on SSL configuration, see the chapter "Security."

Microsoft SQL Server Connection Management

Select the Microsoft SQL Server database type to add a Microsoft SQL Server database connection node to the Management Console tree.

Click **Test Connection** to verify that the Dynamic Data Masking service can access the database.

Microsoft SQL Server Connection Parameters

Define the following connection parameters for a Microsoft SQL Server database:

DDM Database Name

Name for the database in the Management Console tree.

Server Address

Server host name or TCP/IP address for the Microsoft SQL Server database.

Note: Verify that there is no firewall that prohibits the Dynamic Data Masking Server from connecting to the database server and port number.

Server Instance Name

The instance name of the Microsoft SQL Server database.

If the Microsoft SQL Server database is configured to use dynamic port allocation, you can enter the Server Instance Name to identify the listener port. If you enter the instance name, you do not need to enter a Server Port number.

Server Port

TCP/IP listener port for the Microsoft SQL Server database. If you enter the Server Port number, you do not need to enter a Service Instance Name.

Optional Parameters

Additional parameters for the Informatica driver for Microsoft SQL Server.

Keystore

Select custom if you have configured a custom keystore. Select default if you want to use the default keystore preconfigured for use with Dynamic Data Masking.

DBA Username

User name for the database user account to log in to the Microsoft SQL Server database. The database user must be a privileged user that has SELECT access to all the tables that the client user has SELECT access to. This parameter is valid for the default keystore.

DBA Password

Password for the database user. This parameter is valid for the default keystore.

Key Store Name

Name of the custom keystore, defined in the `ddm.security` file. This parameter is valid for custom keystores.

Alias

Alias name for the custom keystore. For CyberArk accounts, the alias name was defined during creation of the CyberArk account. This parameter is valid for custom keystores.

SSL

Select to enable SSL communication between the database and the Dynamic Data Masking Server. For more information on SSL configuration, see the chapter "Security."

CHAPTER 5

Rules

This chapter includes the following topics:

Rules Overview

A rule contains the conditions and actions that the Rule Engine uses to process a request. Connection rules process application connection requests. Security rules process SQL statements. You create and define rules to manage the SQL requests that the client or application sends to the target database.

A rule defines connection criteria and masking techniques. The Rule Engine uses connection criteria to forward requests and masking techniques to mask data. Rules can be connection rules or security rules, placed in a rule tree. The organization of the rule tree determines the order in which the Rule Engine applies the rules. You can create and edit rules within the Management Console.

Rule Components

A rule consists of a matcher, an action, and a processing action. Each rule component defines how the Rule Engine identifies and processes a request to the database.

The Rule Engine applies a connection rule to incoming connection requests and applies security rules to SQL statements. A connection rule defines how the Dynamic Data Masking service establishes a connection with the application. A security rule defines the conditions and masking rules that the Rule Engine applies to the SQL statement request. The Rule Engine applies a security rule if you configure a connection rule to apply a rule set.

A rule consists of the following components:

Matcher

Defines the criteria that the Rule Engine uses to identify a match.

Action

Defines the action that the Rule Engine applies to the request.

Processing action

Defines the action that the Rule Engine applies to the request after the Rule Engine applies the rule. The processing action manages how the Rule Engine processes the request through the rule tree. A processing action can specify that the Rule Engine does not process further rules in the rule tree or that the Rule Engine continues to evaluate other rules.

Rule Trees

A rule tree represents the organizational structure of rules and rule folders. The position that you assign a rule or rule folder within the rule tree determines the order in which the Rule Engine processes the rule. You build conditional relationships between rules through the rule tree.

A rule tree can be a connection rule tree or a security rule tree. Each rule tree uses a system of folders and rules to determine the hierarchical order for rule processing.

When the Dynamic Data Masking Server receives a connection request, the Rule Engine parses the request through the connection rule tree. If the connection rule assigns a security rule set, then the Rule Engine parses the SQL request through the security rule tree. The security rule set defines the security techniques that the Rule Engine applies to rewrite the SQL statement.

Rule Tree Components

Connection rules and security rules work together to define when and how data is masked.

Use the following components to identify and manage application requests:

Rule

The conditions and actions that you want to apply to a request. A rule can be a connection rule or a security rule. You can create an individual rule or create a rule as part of a rule folder.

A rule consists of a matcher, action, and processing action.

Rule folder

A rule that uses the Folder rule action. You can use a rule folder to group conditional rules. The Rule Engine processes the contents of a rule folder hierarchically.

A connection rule folder contains connection rules. A security rule folder contains security rules.

Connection rule

A rule that defines the criteria that the Rule Engine uses to identify the target database for the request. A connection rule consists of a matcher and an action that you define to identify and route a connection request from an application.

Connection rule tree

The connection rule tree defines the order in which the Rule Engine processes connection rules. The connection rule tree contains all the connection rules that you define for the target databases. The Rule Engine processes the first rule or rule folder in the connection rule tree and stops at the end of the rule tree or when there is a stop processing action.

Security rule

A rule that defines the criteria that the Rule Engine uses to parse and alter the SQL statement request. A security rule consists of a matcher and action that you define to identify and mask a SQL request.

Security rule set

A security rule set is a container for security rules. You use rule folders to organize and nest rules within the rule set. A security rule set can contain multiple rule folders. The Rule Engine processes the SQL statement through the rule set until the Rule Engine encounters a stop processing action.

Security rule tree

Each security rule set has an individual security rule tree. The security rule tree defines the order in which the Rule Engine processes security rules. The security rule tree contains the security rules for a particular security rule set. The Rule Engine processes the first rule or rule folder in the security rule tree and stops when there is a stop processing action.

Security Rule Sets

A rule set is a collection of security rules. Create a rule set to group security rules that you want the Rule Engine to apply to SQL request statements. Assign the rule set to a connection rule. The Rule Engine applies the rule set if the connection request matches the conditions that the connection rule defines.

A security rule set can contain a combination of rules that perform different tasks. You can add security rules that mask data, block requests, rewrite the SELECT statement, or replace a part of the SELECT statement. To organize rules within a rule set, you use rule folders to group security rules that apply the same action. For example, group rules that use the mask action in one rule folder, and group rules that use the block action in a different rule folder.

Creating a Security Rule Set

Create a security rule set to group security rules that share a relational link.

1. In the Management Console, click on a domain node in the rule tree.
2. Click **Tree** > **Add Rule Set**.

   The **Add Rule Set** window appears.
3. Enter a name for the security rule set and click **OK**.

   The security rule set appears inside the rule tree in the Management Console.

You can add security rules to the rule set.

Rule Folders

A rule folder is a container for rules that share conditional relationships. You can rename, reconfigure, move, cut, copy, paste, delete, disable, and enable a rule folder. Create rule folders to organize related rules and define the order in which the Rule Engine applies them.

A rule folder can contain connection rules or security rules. A connection rule folder groups rules that you apply to connection requests. A security rule folder contains rules that you apply to SQL request statements.

To create a rule folder, specify the folder action for the rule. Within the rule folder, create relational rules that help the Rule Engine identify, match, and rewrite requests. Before you can add rules to a folder, you must outline the relationships between the rules that you want the folder to contain.

You can group rules that share the same purpose. For example, group masking rules together in a rule folder and group access control rules in another rule folder.

Note: When you create a rule folder, you must set the processing action to **Continue**. When the Rule engine encounters a continue processing action, the Rule Engine processes the request through the rules that the folder contains.

Rule Management

You can rename, reconfigure, move, cut, copy, paste, delete, disable, and enable a rule. When you make changes to a rule, you must update the rule tree for the change to take effect.

When you create, edit, or add a connection rule, you must restart the current session with the application before the Rule Engine can apply the connection rule. Updates to a security rule take effect immediately. You do not need to start a new session for the Rule Engine to apply a security rule.

You can move a rule to change the position of the rule in the rule tree. You can move a rule folder to change the position of the folder in the rule tree. You cannot move a rule into or out of a folder. Move a rule to change the order in which the Rule Engine applies the rule.

You can enable or disable a rule or rule set. By default, the rule or rule set is enabled. When you enable a rule or rule set, the Rule Engine applies the rule or rule set to the request. When you disable a rule, the Rule Engine skips the rule or rule set and applies the next rule or rule set in the rule tree.

You can delete a rule or rule folder from the rule tree. When you delete a rule folder, you delete the content that the rule folder contains. You cannot undo the changes after you delete a rule or rule folder from the rule tree.

Editing a Rule

You can edit the matcher, action, processing action, and name for any rule.

1. Open the **Rule Editor** for connection rules or security rules.
2. Click on a rule in the rule tree.
3. Click **Edit**.

   The **Edit** window appears.
4. Make the changes that you want to the rule components.
5. Click **OK**.
6. Select **File** > **Update Rules**.

   The rule tree is updated.

INDEX