Cisco Data in Motion Installation Guide, Release 1.0.1

February 25, 2015

This document provides the information that is required to understand and install the Cisco Data in Motion (DMo) software.

This document is intended for developers or system administrators who want to install the Cisco Data in Motion software components. It assumes that you have knowledge or experience with Cisco Data in Motion, system administration, and the following:

- Red Hat Enterprise Linux (RHEL)
- UNIX and/or Linux File System
- Red Hat Package Manager (RPM)
- Virtual Machine (VM)
- Open Virtualization Appliance (OVA)
- Open Virtualization Format (OVF)

This document includes these topics:

Minimum Supported Hardware Platform

Cisco Data in Motion requires the following minimum hardware components:

- Red Hat Enterprise Linux (RHEL) 6.x (64-bits) Operating System (OS)
- Cisco Unified Computing System (UCS)
- 2vCPU cores, 4GB vRAM (OVA Configuration for UCS-C/E)

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- VMWare ESX or ESXi 5.0+ (Virtualization Platform)
- Oracle VirtualBox version 4.3.x+ (Virtualization Platform)

Installing Cisco Data in Motion

Cisco Data in Motion (DMo) software can be configured and installed onto Red Hat Enterprise Linux (RHEL) 64-bits Operating Systems (OS) running as a Virtual Machine (VM) either on VMWare ESX/ESXi 5.0+ or Oracle's VirtualBox version 4.3.x or higher.

The OVA has been preconfigured to automatically startup the Data in Motion software as a background process and automatically stop the DMo process when RHEL OS is shutting down.

To install and set up the Cisco Data in Motion software for RHEL 6.x running as a VM, follow these steps:

Procedure

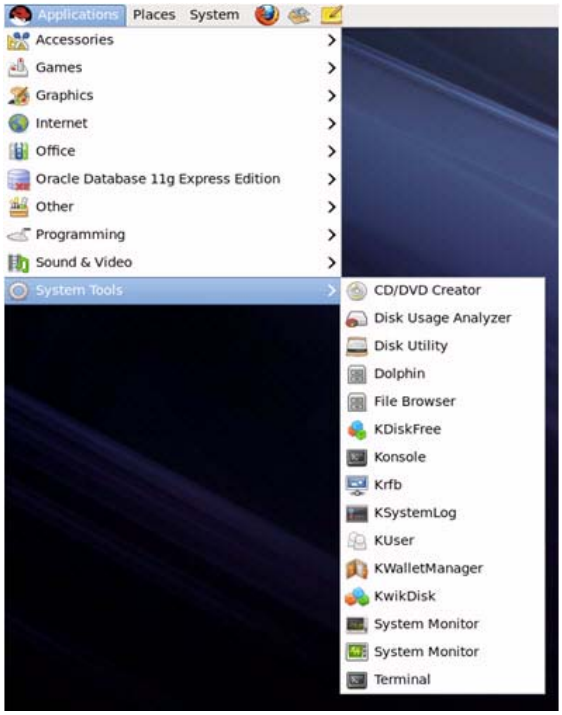
Step 1 Download a copy of the Red Hat Enterprise Linux (RHEL) 6.x OVA.

Step 2 Import the rhel64_64bits.ova using either VMWare ESX/ESXi or Oracle's VirtualBox.

Step 3 Start the RHEL VM instance and notice that the VM is preconfigured with 2 GB RAM and 2 CPU allocations.

Step 4 A default Linux user account has been set up with userid - localadmin and password - cisco911. Login with these credentials. After successfully authentication on RHEL, open an instance of the UNIX/Linux Terminal shell window by clicking **Applications > Systems Tools > Terminal**, as shown in Figure 1.

Figure 1 RHEL Terminal Window



Step 5 On the Terminal shell window, type the following processor status UNIX/Linux command to list whether the Data in Motion software is already running as a background process:

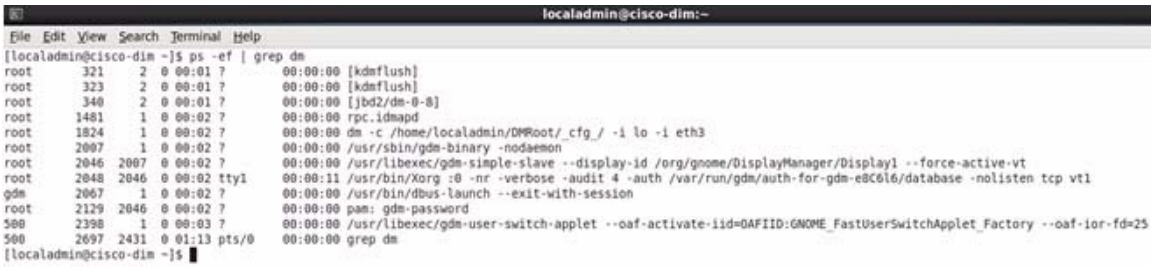
ps -ef | grep dm

The processor command should return at least the following indicator that the Data in Motion software is running as a background process:

```
dm -c /home/localadmin/DMRoot/cfg/ -i lo -i eth0
```

See Figure 2 for an example.

Figure 2 Status Information



Note Your VM might allocate a different Ethernet identifier than eth0 depending on how the OVA was installed.

Step 6 If Data in Motion did not automatically startup in the background, execute the following UNIX/Linux shell script as sudo root account access using same password cisco911.

sudo /etc/init.d/dm_start_stop start

Note Linux account user localadmin has been automatically granted sudo root access to execute certain UNIX/Linux commands that is needed by Data in Motion software.

Alternatively, the /etc/init.d/dm_start_stop shell script can also stop and restart as follows:

sudo /etc/init.d/dm_start_stop stop

sudo /etc/init.d/dm_start_stop restart

Usage: /etc/init.d/dm_start_stop {start|stop|restart}

Step 7 (Do not attempt this step without receiving guidance from Cisco Support.) The OVA may not always have the latest version of the Data in Motion software preinstalled. The easiest way to upgrade to the latest DMo package is by installing the RPM package (e.g. dm-1.0-x.el6.x86_64.rpm, where x denotes the Data in Motion package build number and yyyyyy denotes the current git hash identifier).

To upgrade the Data in Motion software package, download the latest copy of the Data in Motion RPM. You can contact the sales/support team to obtain this copy.

Once you obtain the RPM, run the following command on the terminal:

sudo rpm -Uvh dm-1.0-16_3dc0924.el6.x86_64.rpm

[sudo] password for localadmin: cisco911

```
Preparing...
        ########################################[100%]
```

```
   1:dm ##########################################[100%]
Completed Data in Motion RPM install.
```

Step 8 You can create specific user contexts by using the following UNIX/Linux shell provided located at /home/localadmin/crudDMUserContext

Note A context is an associated collection of related Data Definitions that can be accessed by an authorized set of users. Each user of a context has a separate login username and password for security authentication and authorization.

The contexts are created under the directory structure /home/localadmin/DMRoot/contexts and this location is configurable. (See the default XML configuration file located at /home/localadmin/DMRoot/cfg/dm.cfg for more details). Changing default context paths is an advanced configuration. Consult Cisco Support before changing default context paths.

Usage: **crudDMUserContext --config </path/to/_cfg_>**

--create [contextUser] [password] [new password]

--modify [contextUser] [password] [new password]

--delete [contextUser] [password]

--remove [contextUser] [password]

--verify [contextUser] [password]

--resetFactory [contextUser] [password]

- Create Context—Allows the DMo Administrator to add a context user with a global password and configurations.
- Modify Context—Allows the DMo Administrator to update username and password within a given context based on existing and new password.
- Delete Context—Allows the DMo Administrator to disable the context and prevent users from logging in. You may be able to recover the contents of the context after this operation. (Request guidance from Cisco support.)
- Remove Context—Allows the DMo Administrator to remove a context (e.g. username and password) alltogether. You cannot recover the contents of the context after this operation.
- Verify Context—Allows the DMo Administrator to verify the password within a given context.
- Reset Factory—Allows the DMo Administrator to resets to default factory settings for a given user context (e.g. username and password) by recreating all the directory structure. This is useful for refreshing the given context user if needed.

For example, to create a new user context called "Peter" with password "mySecretPasswd123," the UNIX/Linux using the crudDMUserContext shell script looks like the following:

/home/localadmin/crudDMUserContext --config
/home/localadmin/DMRoot/_cfg_/ --create Peter
mySecretPasswd123

If successful, the output displays the following:

```
Setting config _cfg_ path to: /home/localadmin/DMRoot/_cfg_/

GENKEY: Command Line Interface (CLI) System Utility
XDB Version B1.1-01
Copyright tigerme.com 2007-2013, U.S.A. Thu Dec 11 01:36:32 2014
```

Note Optionally, you can use the client API HTTP GET command to create/modify/delete (see the definitions above) a context. You will need to include HTTP basic authorization header with the username/password combination as localadmin/cisco911. The URL patterns are as follows -

Create Context - https://<ipaddr>:<configport>/*/C/<context name>/<context password>
Update Context- https://<ipaddr>:<configport>/*/U/<context name>/<new password>
Delete Context - https://<ipaddr>:<configport>/*/D/<context name>

Step 9 To run the Java-based SDK for the sensor demo client application that will create a rule called "sensordemo":

Usage: **./sensordemo.sh <srcIPAddr> <srcPort> <destIPAddr> <destPort> <contextUser> <contextPasswd> <JavaKeyStoreFile>**

Example: **./sensordemo.sh 10.0.2.15 8082 10.0.2.15 5001 DMRootCtx ciscoDM123 /home/localadmin/user-java-api /keystore/dmkeystore.jks**

Note The srcIPAddr is the source IP address and the destIPAddr is the IP address of the destination endpoint.

Step 10 Installing the License.

At this point Data in Motion will be running in minimal mode. Although you will be able to setup rules, the rules will not be executed. To make Data in Motion fully functional you will need to install a valid license. You should have received a valid license file along with your purchase of the Data in Motion product. If not, please contact the sales/support team to obtain a license.

Once you obtain the license, copy it to the path /home/localadmin/DMRoot/lic using the following command -

cp <path to downloaded license file> /home/localadmin/DMRoot/lic/

Restart the Data in Motion process for the license to take effect, using the following command -

sudo /etc/init.d/dm_start_stop restart

Note Optionally, you can use the client API HTTP PUT command to upload the license key file. You will need to include HTTP basic authorization header with the username/password combination as localadmin/cisco911

Step 11 To test that the Data in Motion software is running properly, either run the Java or C-based Data in Motion client-side Software Development Kit (SDK) available in the OVA.

The Java client SDK is located at the /home/localadmin/org.eclipse.krikkit/krikkit-java-api/ directory.

The C-based client SDK is located at the directory /home/localadmin/org.eclipse.krikkit/krikkit-c-api/ directory.

Step 12 To run the Java-based SDK for the sensor demo client application that will create a rule called “sensordemo”:

Usage: ./sensordemo.sh <srcIPAddr> <srcPort> <destIPAddr> <destPort> <contextUser> <contextPasswd> <JavaKeyStoreFile>

Example: ./sensordemo.sh 127.0.0.1 443 127.0.0.1 5001 DMRootCtx ciscoDM123 /home/localadmin/user-java-api /keystore/dmkeystore.jks

Note The srcIPAddr is the IP address of the machine running Data in Motion and the destIPAddr is the IP address of the endpoint to which Data in Motion will send events that match a rule. In the above example, we use the localhost for both srcIPAddr and destIPAddr to indicate that Data in Motion runs on the localhost and we want Data In Motion to send events to port 5001 on the localhost.

Step 13 To run the C-based SDK for the sensor demo client application that will create a rule called "sensordemo":

Change directory (cd) to /home/localadmin/org.eclipse.krikkit/krikkit-c-api/tests/

Usage: **./sensordemo <srcIPAddr> <srcPort> <destIPAddr> <destPort> <contextUser> <contextPasswd>**

Example: **./sensordemo 127.0.0.1 443 127.0.01 5001 DMRootCtx ciscoDM123**

Step 14 Check that the sensor demo rule has been created by issuing the following UNIX/Linux commands:

- Change directory (cd) to /home/localadmin/DMRoot/DMRootCtx
- List current directory (ls -l)

The output should have a JSON data file called "sensordemo.json" and a directory called "+sensordemo":

```
total 8
drwx------. 2 localadmin localadmin 4096 Jan 17 13:28 +sensordemo
-r--------. 1 localadmin localadmin  358 Feb 13 01:51 sensordemo.json
```

Alternatively, you can check the Data in Motion default log file in the /home/localadmin/DMRoot/_log_ directory.

Data in Motion Configuration UI

The OVA comes prepackaged with a simple UI with which you can configure rules on Data in Motion. The OVA uses nodejs to run the UI. You can access the UI, locally on the OVA, at http://localhost:8000.

Note If you require the UI to be accessible from outside the OVA, you need to setup appropriate NAT entries form the host to port 8000 of the OVA.

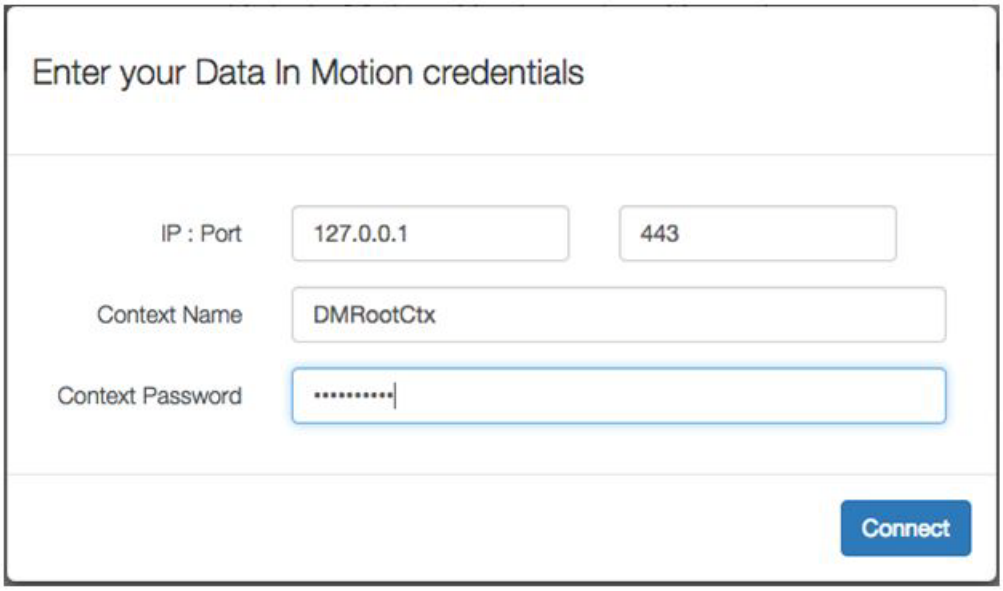
The following steps describe how you can connect to the Data in Motion instance and create a rule.

Procedure

Step 1 On the browser, go to the URL http://localhost:8000. You will be asked for login information. Enter the IP address of the machine running Data in Motion (this example demonstrates logging into the DMo instance running on the localhost) and the port on which Data in Motion listens for configurations (the default is 443).

Also provide the context name and password you want to login to. Figure 3 demonstrates logging into the default context. DMRootCtx (the default password for this context is 'ciscoDM123').

Figure 3 Logging In to the Default Context

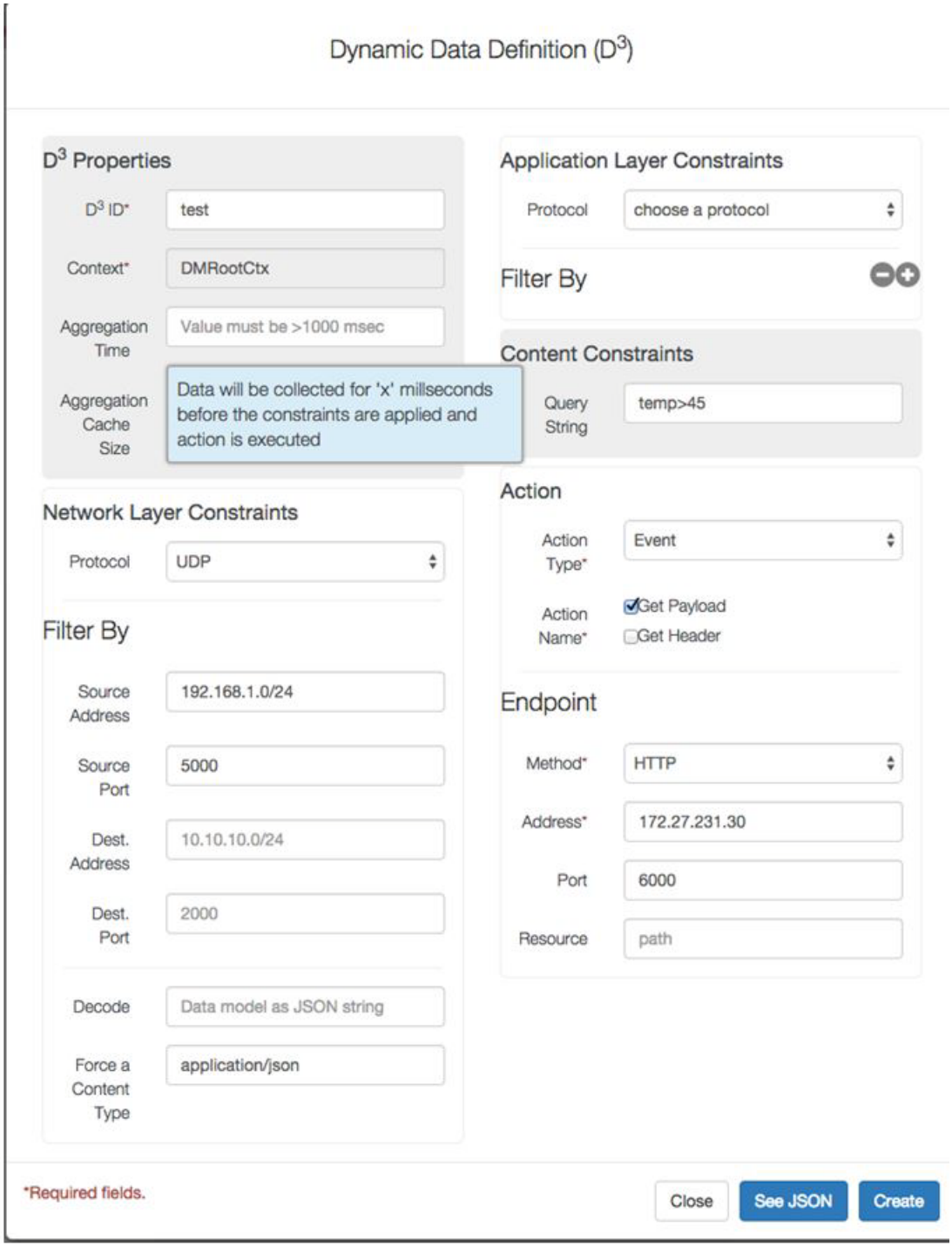


Step 2 Once logged in, you will see all the rules that have been installed in this context.

Step 3 You can add a rule by clicking on the 'Add D3' button on the top right of the screen.

Step 4 Figure 4 shows the rule creation window. There are tooltips for each field that describe what parameters the field takes and how it must be used. This figure shows a simple rule named test to capture UDP packets whose source subnet is 192.168.1.0/24 and source port is 5000, apply a json parser on the context and generate an event if the content has “temp” > 45. The event will be sent to the destination 172.27.231.30 on port 6000 using the HTTP PUT method.

Figure 4 Rule Creation Window



Step 5 You can view how the UI converts this to the Data in Motion JSON rule representation by clicking the **See JSON** button. Figure 5 shows the JSON for the above rule

Figure 5 JSON for Rule

Step 6 Click the **Create** button to add the rule to your context. Once added, you will be able to view the rule.

Data in Motion Command Line

Note The information in this section is for advanced users only.

The RHEL OVA installs the Data in Motion binary executables at the following locations:

- /usr/sbin/dm - Data in Motion software

  Synopsis: <-i en1> -d (packet dump) -c <config directory> -b (rebuild rules)

  – -i—Allows the DMo Administrator (e.g. run as root user or as sudo root) to define the network interfaces or devices to bind to with a maximum of 5 (e.g. -i lo -i eth1 -i eth2 -i eth3 -i eth4).

  - -d—Optionally, allows the DMo Administrator to print the packet-level dump information that is useful for verbose and debugging purposes.
  - -c—Optionally, allows the DMo Administrator to set the configuration directory containing one or more configuration files. Default configuration directory is set to "/Documents/_cfg_/".
  - -b—Optionally, allows the DMo Administrator to rebuild all the rules that is referenced under the configuration directory structure.
- /usr/sbin/gnkey - Creates, Updates, Verifies and Deletes Context Users

  Synopsis gnkey --with arguments:

  --config [configs] --create [context] [password]

  --config [configs] --modify [context] [password] [new password]

  --config [configs] --delete [context] [password]

  --config [configs] --remove [context] [password]

  --config [configs] --verify [context] [password]

The UNIX/Linux shell script /home/localadmin/crudDMUserContext utilizes the /usr/sbin/gnkey to create, update, verify and delete context users.

Data in Motion Configuration

The default Data in Motion configuration file uses an XML-based format constructs with the following definitions:

- _mem_prefix_—Sets the path to the data streams.
- _dci_filter_—Sets the packets filter type (e.g. UDP, TCMP, ICMP)
- _ctx_prefix_—Sets the default absolute path name for root context. No chdir occurs for path.
- _log_prefix_—Sets the default absolute pathname for log directory.
- _adm_prefix_—Sets the default admin prefix for Cisco FLEXlm license keys.
- _filter_url_—Sets the default rule name for URL filter. Must set context and schema.
- _ip_network_—Sets the IP address of node to connect with as the node synchronization.
- _MAXtimeout_—Sets the client timeout in floating point seconds.
- _listenPort_—Sets the port number to listen from.
- _configPort_—Sets the port number to configure from.
- _auth_basic_—Sets the Base64 encoding of pair value token HTTP Basic Authentication header.
- _crt_prefix_—Sets the path location to X.509-compliant SSL certificate.
- _key_prefix_—Sets the path location to X.509-compliant SSL key.

The following shows the syntax of a sample Data in Motion configuration file, which is located by default at /home/localadmin/DMRoot/cfg/dm.cfg:

```
<_filter_url_>
  FitlerURL
</_filter_url_>

<_mem_prefix_>
  /home/localadmin/DMRoot/mem
</_mem_prefix_>
```

```
<_ctx_prefix_>
  /home/localadmin/DMRoot/DMRootCtx
</_ctx_prefix_>

<_log_prefix_>
  /home/localadmin/DMRoot/_log_
</_log_prefix_>

<_crt_prefix_>
  /home/localadmin/DMRoot/cert/dm.crt
</_crt_prefix_>

<_key_prefix_>
  /home/localadmin/DMRoot/cert/dm.key
</_key_prefix_>

<_adm_prefix_>
  /home/localadmin/DMRoot/lic
</_adm_prefix_>

<_ip_network_>
  127.0.0.1
</_ip_network_>

<_listenPort_>
  8443
</_listenPort_>

<_configPort_>
  443
</_configPort_>
```

Note Changing the default XML configurations in the dm.cfg file must be done only by an advanced user.

.