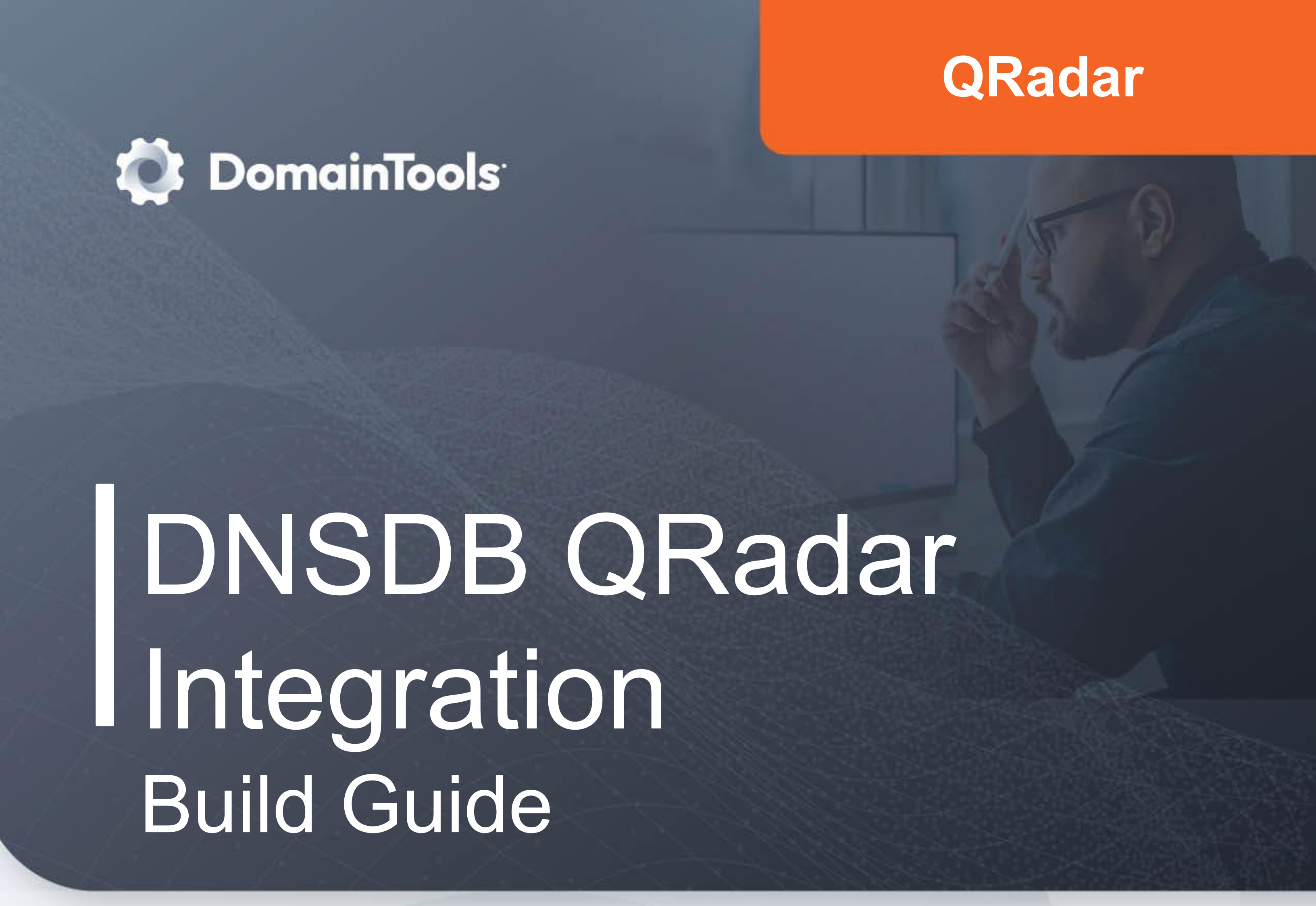
QRadar

DomainTools



DNSDB QRadar Integration

Build Guide

1. Prerequisites

QRadar SDK:

- Download and install QRadar SDK from here
- Installation guide is available here

❖ ***Note 1:*** Install QRadar SDK as a non-root user
❖ ***Note 2:*** Docker is a Prerequisite for QRadar SDK

Once QRadar SDK is correctly installed, you should be able to run the command: `qapp` for the user.

QRadar Instance:

In order to deploy and export a package, a QRadar instance must be available.
Note down the QRadar console IP/Hostname, username, password.

2. Packaging with SDK

We will first package the app using SDK installed earlier.

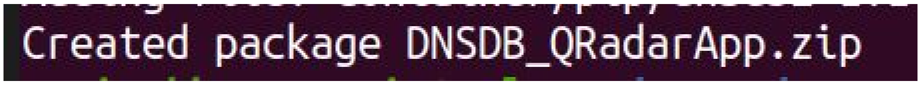
1. Download the Application Source code from github and navigate to the `DNSDB_QRadarApp_Source` folder.
2. While in this folder, issue the below command

```
qapp package -p <package_name>
```

`Example:`

```
qapp package -p DNSDB_QRadarApp.zip
```

With this, a new ZIP package file wil be created in the current folder.
Command output:



```
Created package DNSDB_QRadarApp.zip
```

Deploying to QRadar

Follow the procedures below to Deploy the Package on a QRadar Instance.

Using CURL command

QRadar provides an API to POST a Application creation task.
We will be using this API endpoint to create a new application with the Package file.

Command:

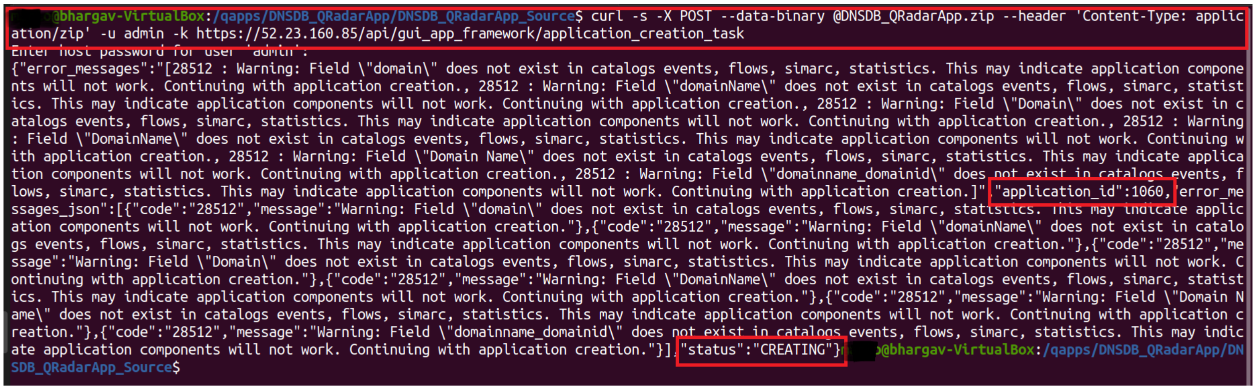
```
curl -s -X POST --data-binary @<Package filename> --header \
    'Content-Type: application/zip' -u <QRadar Username> -k \
    https://<QRadar Console
IP/Hostname>/api/gui_app_framework/application_creation_task
```

- <Package filename> : Filename of package create with qapp command earlier.
- <QRadar Username> : Username to access QRadar. Mostly `admin`
- <QRadar Console IP/Hostname> : IP/Hostname of the QRadar instance to deploy this package to.

Once this command is executed, it will prompt for a password for the specified user.

If the App package is posted successfully, it will return a message with status as `creating` in response. Make a note of the App ID from this response.

Response will look something like this



```
[redacted]@bhargav-VirtualBox:/qapps/DNSDB_QRadarApp/DNSDB_QRadarApp_Source$ curl -s -X POST --data-binary @DNSDB_QRadarApp.zip --header 'Content-Type: applic
ation/zip' -u admin -k https://52.23.160.85/api/gui_app_framework/application_creation_task
Enter host password for user 'admin':
{"error_messages":"[28512 : Warning: Field \"domain\" does not exist in catalogs events, flows, simarc, statistics. This may indicate application compone
nts will not work. Continuing with application creation., 28512 : Warning: Field \"domainName\" does not exist in catalogs events, flows, simarc, statist
ics. This may indicate application components will not work. Continuing with application creation., 28512 : Warning: Field \"Domain\" does not exist in c
atalogs events, flows, simarc, statistics. This may indicate application components will not work. Continuing with application creation., 28512 : Warning
: Field \"DomainName\" does not exist in catalogs events, flows, simarc, statistics. This may indicate application components will not work. Continuing w
ith application creation., 28512 : Warning: Field \"Domain Name\" does not exist in catalogs events, flows, simarc, statistics. This may indicate applica
tion components will not work. Continuing with application creation., 28512 : Warning: Field \"domainname_domainid\" does not exist in catalogs events, f
lows, simarc, statistics. This may indicate application components will not work. Continuing with application creation.]","application_id":1060,"error_me
ssages_json":[{"code":"28512","message":"Warning: Field \"domain\" does not exist in catalogs events, flows, simarc, statistics. This may indicate applic
ation components will not work. Continuing with application creation."},{"code":"28512","message":"Warning: Field \"domainName\" does not exist in catalo
gs events, flows, simarc, statistics. This may indicate application components will not work. Continuing with application creation."},{"code":"28512","me
ssage":"Warning: Field \"Domain\" does not exist in catalogs events, flows, simarc, statistics. This may indicate application components will not work. C
ontinuing with application creation."},{"code":"28512","message":"Warning: Field \"DomainName\" does not exist in catalogs events, flows, simarc, statist
ics. This may indicate application components will not work. Continuing with application creation."},{"code":"28512","message":"Warning: Field \"Domain N
ame\" does not exist in catalogs events, flows, simarc, statistics. This may indicate application components will not work. Continuing with application c
reation."},{"code":"28512","message":"Warning: Field \"domainname_domainid\" does not exist in catalogs events, flows, simarc, statistics. This may indic
ate application components will not work. Continuing with application creation."}],"status":"CREATING"}[redacted]@bhargav-VirtualBox:/qapps/DNSDB_QRadarApp/DN
SDB_QRadarApp_Source$
```

To know the Status of the application creation task, we will use another endpoint.

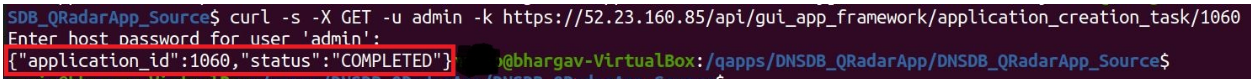
Issue below command:

```
curl -s -X GET -u <QRadar Username> -k https://<QRadar Console
IP/Hostname>/api/
gui_app_framework/application_creation_task/<Application ID>
```

Once this command is executed, it will prompt for a password for the specified user.

- <Application ID> : Application ID from response of application creation task command above.

If app is installed successfully, the response should look like below.



```
SDB_QRadarApp_Source$ curl -s -X GET -u admin -k https://52.23.160.85/api/gui_app_framework/application_creation_task/1060
Enter host password for user 'admin':
{"application_id":1060,"status":"COMPLETED"}[redacted]@bhargav-VirtualBox:/qapps/DNSDB_QRadarApp/DNSDB_QRadarApp_Source$
```

After this step, check whether Application is running on the QRadar Instance manually.

Exporting App Package

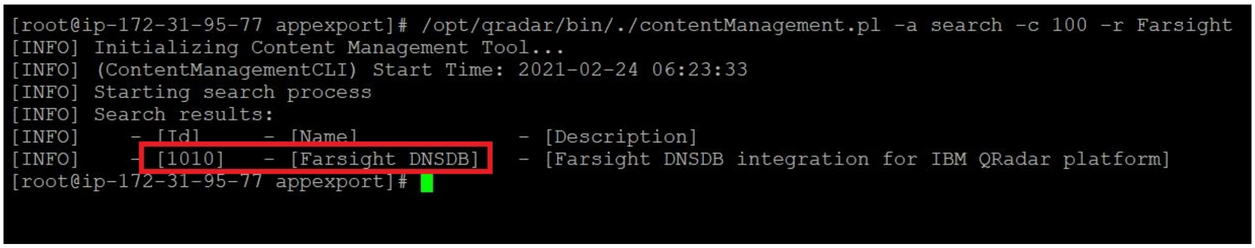
Once the App is installed on the QRadar instance and working as expected, we will Export this App from that QRadar Instance. This exported zip will then be used to Submit on the IBM App Exchange Hub.

To Export the Application, login to QRadar Instance via `SSH` and issue below commands.

- Search for the content ID of the installed application using Content management tool command below.

```
/opt/qradar/bin/./contentManagement.pl -a search -c 100 -r Farsight
```

This will list all the Application installed with name matching regex Farsight Response will look like below.



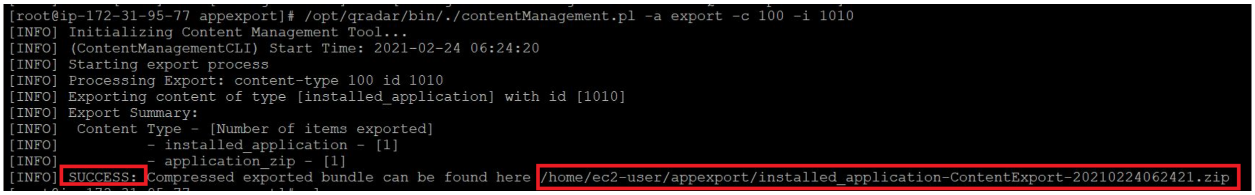
```
[root@ip-172-31-95-77 appexport]# /opt/qradar/bin/./contentManagement.pl -a search -c 100 -r Farsight
[INFO] Initializing Content Management Tool...
[INFO] (ContentManagementCLI) Start Time: 2021-02-24 06:23:33
[INFO] Starting search process
[INFO] Search results:
[INFO]     - [Id]      - [Name]            - [Description]
[INFO]     - [1010]    - [Farsight DNSDB]  - [Farsight DNSDB integration for IBM QRadar platform]
[root@ip-172-31-95-77 appexport]#
```

Make a note of this Content ID for exporting the app.

2. Export the Application using content ID from above step using below content management tool command:

```
/opt/qradar/bin/./contentManagement.pl -a export -c 100 -i <Content
Identifier ID>
```

Once the Script runs successfully, it will save a compressed Application package in the folder the command is run from.



```
[root@ip-172-31-95-77 appexport]# /opt/qradar/bin/./contentManagement.pl -a export -c 100 -i 1010
[INFO] Initializing Content Management Tool...
[INFO] (ContentManagementCLI) Start Time: 2021-02-24 06:24:20
[INFO] Starting export process
[INFO] Processing Export: content-type 100 id 1010
[INFO] Exporting content of type [installed_application] with id [1010]
[INFO] Export Summary:
[INFO]  Content Type - [Number of items exported]
[INFO]          - installed_application - [1]
[INFO]          - application_zip - [1]
[INFO] SUCCESS: Compressed exported bundle can be found here /home/ec2-user/appexport/installed_application-ContentExport-20210224062421.zip
```

This is the Package that needs to be submitted to IBM after adding manifest.txt and signing the Application.