Subject: Internal ITRM SAS Note

Author: Joe Hatcher

Date: May 8, 2018

SAS Note Title: IT Resource Management Adapter for VMware vCenter and VMware Data Acquisition – Accessing the vPostgres Database

In SAS IT Resource Management 3.8, instructions were provided to allow Customers to Enabling Access to the VMware vCenter Server Appliance (vCSA) Postgres Database. These instructions were provided with the following caveat:

VMware vCSA also supports an embedded Postgres database option. The embedded Postgres database is implemented by VMware as a closed system to which access instructions are not documented. Though not recommended by VMware, it is possible to use the IT Resource Management Adapter for VMware vCenter to read data from the vCenter Postgres database.

In April, 2018 the ITRM Product team became aware that when Customers followed the special instructions to access the vCenter vPostgres database, a TLS 1.0 security vulnerability was raised. This vulnerability occurs because of the vPostgres database implementation by VMware when that database is accessed outside of the VMware Firewall. For this reason, the ITRM text providing instructions for the IT Resource Management Adapter for VMware vCenter to read the vCenter vPostgres database was removed.

When an IT Resource Management Customer contacts SAS and requires that the IT Resource Management Adapter for VMware vCenter be used to access the VMware or VMware vCenter Server Appliance vPostgres database, the following steps can be taken.

1. Recommend that the Customer use a version of vCenter or the vCenter Server Appliance that supports the use of an external Oracle or Microsoft SQL Server database:

|  |  |  |
| --- | --- | --- |
| **vCenter Server Releases** | **vCenter Server Appliance Releases** | **External Databases Available** |
| Prior to 5.5 |  | Oracle, Microsoft SQL Server, IBM DB2  |
|  | 5.0 | IBM DB2, Oracle |
|  | 5.01 – 6.0 | vPostgres, Oracle |
| 6.0 – Current |  | Oracle, Microsoft SQL Server, vPostgres |
|  | 6.5 – Current | vPostgres |

1. Inform the Customer that the VMware vCenter vPostgres database is implemented as a closed system to which access instructions are not documented.
2. Inform the Customer that a method can be used to open the vCenter vPostgres database for external access including access by the IT Resource Management Adapter for VMware vCenter.
3. Inform the Customer that using the method to open the vCenter vPostgres database also exposes the customer to security risks associated with the use of TLS 1.0.
4. Provide the following instructions:

**Enabling Access to the VMware vCenter Server Appliance (vCSA) Postgres Database**

**Introduction to Enabling Access to the vCSA Postgres Database**

**Background**

SAS IT Resource Management provides access to external vCenter databases through SAS Access to Oracle and SAS Access to Microsoft SQL Server engines. These engines access the vCenter database in Read-Only mode and copy the tables and views that are needed by SAS IT Resource Management. Customers typically configure SAS IT Resource Management to access their operational vCenter external databases directly through some create mirrored copies of the vCenter database.

**Note:**Even for very large vCenter databases, SAS Read-Only access can copy the necessary tables in only few minutes.

Starting with vSphere 5.0U1, vCSA provides an option to use vPostgres (a VMware-flavored PostgreSQL) as its embedded database implemented as a closed system. For that reason, VMware publishes no guidance on how the vCenter Postgres database can be accessed directly or mirrored. In exploring the vCSA embedded PostgreSQL database however, the SAS IT Resource Management team discovered a method that, though not sanctioned by VMware, enables the adapter to connect to the vCSA vPostgres server.

**How to Enable Remote Access to the PostgreSQL Server and Collect Raw Data for Input to SAS IT Resource Management**

**Enabling Remote Access to the PostgreSQL Server**

To connect to the database remotely, perform the following steps:

1. Modify the Postgres configuration to allow remote access.
2. Modify VMware's firewall to allow incoming Postgres connections.
3. Create the read-only Postgres user.
4. Check the database connection.

**CAUTION:**

**These procedures are not supported by VMware.**

However, the instructions were successfully tested using VMware 6.5 and 6.0. They also work using VCSA 5.5.

**Modify the Postgres configuration to allow remote access.**

1. To enable your IP to connect to the PostgreSQL server, enter this command:

vim /storage/db/vpostgres/pg\_hba.conf

Then, add the following code to the bottom of that file:

host all 1.2.3.4/24 md5

In this code, replace *1.2.3.4/24* with the actual IP address or range of addresses (for example, *192.168.1.0/24*). Alternatively, replace *1.2.3.4/24* with the server instance or ITRM server from which you want to access the database and run the SAS IT Resource Management adapter.

1. To ensure that the listen\_addresses directive is properly configured, enter this command:

vim /storage/db/vpostgres/postgresql.conf

**Note:**If this directive is not present, then add the following code to the file:

listen\_addresses = '\*'

1. To restart Postgres to apply changes, enter this command:

/etc/init.d/vmware-vpostgres restart

If the Postgres service does not restart properly, you can access the database connection errors by using the PGAdmin tool. For information about possible error messages, navigate to “Connection errors” at this location: https://www.pgadmin.org/svnrepo/pgadmin3-1.20/docs/en\_US/\_build/html/connect-error.html#connect-error.

To start (not restart) the Postgres Services, use following commands:

/opt/vmware/vpostgres/9.4/bin

sudo -u vpostgres ./pg\_ctl -D /storage/db/vpostgres status

sudo -u vpostgres ./pg\_ctl -D /storage/db/vpostgres stop -m fast

sudo -u vpostgres ./pg\_ctl -D /storage/db/vpostgres start

**Modify VMware's firewall to allow incoming Postgres connections.**

1. Enter this command:

vim /etc/vmware/appliance/firewall/vmware-vpostgres

Then make sure that this file contains the following code:

 {

 "firewall": {

 "enable": true,

 "rules": [

 {

 "direction": "inbound",

 "protocol": "tcp",

 "porttype": "dst",

 "port": "5432",

 "portoffset": 0

 }

 ]

 },

 "internal-ports": {

 "rules": [

 {

 "name": "server\_port",

 "port": 5432

 }

 ]

 }

 }

1. To reload the firewall, enter this command:

/usr/lib/applmgmt/networking/bin/firewall-reload

**Create the read-only Postgres user.**

1. Log on to Postgres as the superuser account.
	* For the 6.0 database version, enter this command:

/opt/vmware/vpostgres/9.3/bin/psql VCDB -U postgres

* + For the 6.5 database version, enter this command:

/opt/vmware/vpostgres/9.4/bin/psql VCDB -U postgres

1. Create the role and grant the minimum necessary privileges by using the following SQL statements:
* create role "vcenterVA\_RO1" login password 'my\_password';
* GRANT CONNECT ON DATABASE "VCDB" TO "vcenterVA\_RO1";
* GRANT USAGE ON SCHEMA vc TO "vcenterVA\_RO1";
* GRANT SELECT ON ALL TABLES IN SCHEMA vc TO "vcenterVA\_RO1";
1. As an alternative to the previous step, you can use the randomly generated password for your database user. To do so, navigate to/etc/vmware-vpx/vcdb.properties.

In this file, you can find the database user name *vc* and its password.

***Example Showing the User Name and Password***



**Check the database connection.**

After the previous steps are completed successfully, use the PGAdmin tool to check the database connection. To do so, perform the following steps:

1. Open PGAdmin and register the new server to establish a new connection to the database.
2. Specify values in the **Name** and **Host** fields. (Enter the user name and password that you used when creating the Postgres user in the previous list of steps.)
3. Deselect the **Store Password** check box.

***Register the New Server***



**Note:**Attempting to connect from an external machines or an IP address cannot work without modification to postgresql.conf and pg\_hba.conf. For information about making the required modifications, see [Modify VMware's firewall to allow incoming Postgres connections.](http://go.documentation.sas.com/?cdcId=itrmcdc&cdcVersion=3.8&docsetId=itrmxag&docsetTarget=n0yj6vage9x64tn1c91hyznou7sd.htm&locale=en#p1nvhpx08qg6pwn1n8bp7vx0gjar). For information about possible error messages, navigate to “Connection errors” at this location: https://www.pgadmin.org/svnrepo/pgadmin3-1.20/docs/en\_US/\_build/html/connect-error.html#connect-error.

**Collecting Raw Data for Input to SAS IT Resource Management**

**Note:**You can access the vCenter Server Appliance Postgres database for use by SAS IT Resource Management in the same way it accesses these vCenter external databases. For more information, see [VMware vCenter - Accessing Data](http://go.documentation.sas.com/?cdcId=itrmcdc&cdcVersion=3.8&docsetId=itrmxag&docsetTarget=p0mml68fet1mojn1ho4ae91t3at8.htm&locale=en).

To configure access to VMware raw data in PostgreSQL Server database, perform the following steps: you must obtain information about the database. Then you can configure ODBC on the SAS server and create the SAS library for the VMware raw data.

1. Configure ODBC on the SAS server.
2. Create the VMware Rawdata SAS Library.
3. Create a New External Database Server.
4. Specify a New Authentication Domain.

**Configure ODBC on the SAS Server**

1. Navigate to the **Drivers** tab of the ODBC Data Source Administrator. Verify that the PostgreSQL Server ODBC driver, PostgreSQL ANSI(x64), is available.

***List of ODBC Installed Drivers***



1. Configure the data source.
	1. On the **System DSN** tab, click **Add** to open the **Create new Data Source** window. Select **PostgreSQL Server**.

***Create the New Data Source***



**Note:**The Unicode version of the driver does not work with the SAS IT Resource Management adapter.

* 1. Click **Finish** to create the new data source. The setup screen for the new data source appears.
	2. As shown, below, enter the appropriate information in the following fields:
		1. **Database**
		2. **Server**
		3. **User Name**
		4. **Password**
	3. Click **Test** to verify your entries. Correct any entries that are incorrect.

When the “Connection successful” message appears in the information box, proceed to create the VMware raw data SAS library.

**Create the VMware Rawdata SAS Library**

To create the VMware raw data library, you must first create an ODBC library.

1. Log on as the unrestricted user to SAS Management Console connected to your SAS server. Invoke the **New Library Wizard** to create a new ODBC Library.

***New Library Wizard***



1. Provide the following information. (Click **Next** to navigate through the wizard.)
	* Enter a name for the database server (for example, *VMware*).
	* Enter the library name as *VMware*.
	* Select the SAS Application server.
	* Enter *vmware* in the **libref** field.
2. Click **Advanced Options**. Click **Other Options** to add any database-specific options. Then, click **OK**.
3. On the next screen, click **New** to create a new database server.

**Create a New External Database Server**

1. On the **New Server Wizard** page, enter a name for the database server (for example, *Vmware*).

***New Server Wizard***



1. On the next page, enter the server properties as shown on the following display.

***Server Properties Page of the New Server Wizard***



1. On the next page, specify the ODBC data source. (This name should be one that you specified when configuring the ODBC library.)

***Connection Properties Page of the New Server Wizard***



1. Click **New** to specify the name of the authentication domain. Click **OK**.

***New Authentication Domain***



1. On the next page, review the settings that you entered. Click **Finish** to create the new Database Server.

***Specify the Server and Connection Information***



1. On the next page, review the settings and revise as necessary. Click **Finish** to create the new library.

**Specify a New Authentication Domain**

1. Select**User Manager** and choose the user for whom you want to add the new authentication domain.

**Note:**The new authentication domain can be added for a group, if needed.

1. Select the **Account** tab and click **New** to display the **Edit Login Properties** window.

As shown below, enter the **User ID** and **Password** credentials along with the **Authentication Domain**.

***Edit Login Properties***



1. Click **OK** to complete the specification of the authentication domain. The library VMware is now available. It can be used to specify the **Rawdata** field when you set up a VMware IT Data Mart.