EMC® Storage Monitoring and Reporting

Version 4.0.2

Installation and Configuration Guide

P/N 302-003-453

REV 01

EMC²

Published January 2017

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

CHAPTER 1

Installing the Virtual Appliance

This chapter includes the following topics:

Installing the Storage Monitoring and Reporting vApp

Storage Monitoring and Reporting is installed as an all-in-one virtual appliance (vApp) with a frontend, backend, and collector on a single VM. You deploy the Storage Monitoring and Reporting vApp from an OVF template using vSphere Client.

Before you begin

- Ensure that DRS is enabled.
- Ensure that the ports listed in the *Ports Usage Matrix* are enabled and not blocked by the firewall.
- Gather the following information:
  - vCenter location where you plan to deploy the appliance
  - Datastore that you can use for deployment
  - Static IP address to assign to your appliance
  - Gateway
  - Netmask
  - DNS Servers
- vApp installations require VMware vSphere 5.x or 6.x.
- The vApp is based on SuSE Enterprise Linux 11 SP3.
- The MySQL version included with the product is 5.5.36 MySQL Community Server (GPL)
- The following separate software products are pre-installed with ViPR SRM: ViPR SRM 4.0.2 SOFTWARE IMAGE (453-010-807) and SLES 11 SP3 SW GPL3 OPEN SOURCE SOFTWARE (453-010-808).

Procedure

1. Navigate to the Support by Product page for Storage Monitoring and Reporting(https://support.emc.com/downloads/40532_EMC-Storage-Monitoring-and-Reporting).
2. Click **Downloads**.
3. Download the **Storage Monitoring and Reporting <version number> vApp Deployment** zip file.

   The host being connected to the vCenter should be local to the ESX servers for the quickest deployment. Locate the OVF deployment file on the host running the vCenter client or place the files on the DataStore.
4. Open vSphere Client and connect to the vCenter Server that manages your VMware environment.
5. Select the Resource Pool where you want to deploy the VM for Storage Monitoring and Reporting.
6. Select **File** > **Deploy OVF Template**.
7. In the **Source** step, locate the OVF template file.
8. Click **Next**.

   To save time, deploy the appliance in the same local area network (LAN) that your VMware ESX/ESXi servers share. Deployment across a WAN can take much longer than a local deployment.

9. In the OVF Template Details step, review the details of the loaded OVF file, and then click **Next**.
10. In the **End User License Agreement** step, review the license agreement. Click **Accept**, and then click **Next**.
11. In the **Name and Location** step:
    a. Accept the default name or type a new name for the appliance.
    b. Specify an inventory location for the appliance in your VMware environment.
    c. Click **Next**.
12. In the **Deployment Configuration** step, select **Small**, **Medium**, or **Large** from the **Configuration** drop-down menu.

    Consult the *Performance and Scalability Guidelines* for the recommended configuration for your target environment.
13. Select the host or cluster where you want to run the deployed template, and then click **Next.**
14. Select the destination storage for the virtual machine files, and then click **Next.**
15. In the **Disk Format** step, select the storage space provisioning method, and then click **Next**.

Option	Description
Thin-provisioned format	On-demand expansion of available storage, used for newer datastore file systems.
Thick-provisioned format	Appliance storage that is allocated immediately and reserved as a block.

Note

EMC recommends the **Thin provisioned format** option when the vApp is deployed in a high performance environment.

16. In the **Network Mapping** step, select a destination network that has an IP Pool associated with it for each of the VMs, and then click **Next**.
17. In the **IP Address Allocation** step, choose the IP allocation policy and IP protocol to use, and then click **Next**.
18. In the **Properties** step, provide the values for each of the VMs, and then click **Next**.
19. In the **Ready to Complete** step, review the list of properties for the appliance, and then click **Finish**.

    A status bar opens in vSphere Client showing the deployment progress.
20. After you finish deployment, in the **Deployment Completed Successfully** dialog box, click **Close**.

Starting the vApp

Use vSphere Client to start the vApp.

Procedure

1. In vSphere Client, navigate to the **Host and Cluster** view.
2. From the configured Resource Pool, find the Resource Pool that you selected for the appliance.
3. Click the VM, and then click **Power on the virtual machine** in the right-hand pane.

   After the initial startup and module installations are complete, the system displays the login prompt.

CHAPTER 2

Installing Using the Binary Installer

This chapter includes the following topics:

Installing on Linux

You can install the product on supported Linux hosts.

Before you begin

- Ensure that you have a login with root privileges. This product should only be installed using root and root privileges.
- Ensure that the ports listed in the *Ports Usage Matrix* are enabled and not blocked by a host or network firewall.
- Download the installation file from `support.emc.com`, and place it in a folder (for example `/sw`) on the server.

Procedure

1. Log in to the server as root.
2. Navigate to the `/sw` folder.
3. Change the permissions of the installer.

   For example: `chmod +x <file_name>.sh`
4. Run the installer from the directory.

   For example: `./<file_name>.sh`
5. Read and accept the End User License Agreement.
6. Accept the default installation directory of `/opt/APG` or type another location.

Configuring the user process limits for a Linux installation

Increase the user process limits for the apg user account to a maximum of 65534. This modification enables services to open 65534 files and 65534 processes when needed. This step is required for proper functioning of the core software.

Before you begin

- Make sure you have a login with root privileges.
- The core software installed on a server running Red Hat Enterprise Linux 6, CentOS Linux 6, SUSE Linux Enterprise Server (SLES) 11, or any other supported Linux operating systems.

Procedure

1. Edit (vi) the `/etc/security/limits.conf` file.
2. Insert the following lines for the apg user after the line that starts with <domain>.

   In this example, the user is `apg`.

```
apg   hard  nofile  65534
apg   soft  nofile  65534
apg   hard  nproc   65534
apg   soft  nproc   65534
```

3. Save the file.
4. To verify the changes, type the following command:

```
su apg -c 'ulimit -n -u'
```

```
open files                      (-n) 65534
max user processes              (-u) 65534
```

5. In the `/opt/APG/bin/apg.properties` file, verify that the hostname is a FQDN host name. If the hostname is a shortname, edit (vi) the file to change the hostname to a FQDN.
6. In the `/etc/hosts` file, verify that the first uncommented line is this host's IP-address, FQDN, and shortname. If this is not first uncommented line, edit the file.
7. STOP: Repeat the ViPR SRM installation and configuration process for all of the servers in this deployment before proceeding.
8. To restart the services, type the following commands from the `/opt/APG/bin` directory of the installation. Troubleshoot any service that does not show a status of "running."

   ```
   ./manage-modules.sh service restart all
   ```

   ```
   ./manage-modules.sh service status all
   ```

9. Proceed to Configuring Binary ViPR SRM using Scale Tools.

Installing on Windows Server

You can install the product on supported Windows Server hosts.

Before you begin

- Ensure that the `\tmp` folder is larger than 2.5 GB.
- Ensure that you have a login with system administrator privileges.
- Ensure that the ports listed in the *Ports Usage Matrix* are enabled and not blocked by the firewall.
- Download the installation file from `support.emc.com`, and place it in a folder (for example, `c:\sw`) on the server.

Procedure

1. Navigate to the `c:\sw` folder.
2. Double-click the `.exe` file.
3. Click **Next** on the **Welcome** screen.
4. Read and accept the End User License Agreement. Click **I Agree**.
5. Select the Destination Folder, and then click **Next**.
6. Click **Install**.
7. When the installation is complete, click **Next**.
8. Click **Finish**.
9. In the `Program Files\APG\bin\apg.properties` file, verify that the hostname is a FQDN host name. If the hostname is a shortname, edit the file to change the hostname to a FQDN.

10. In the `c:\windows\System32\drivers\etc\hosts` file, verify that the first uncommented line is this host's IP-address, FQDN, and shortname. If this is not first uncommented line, edit the file.
11. STOP: Repeat the ViPR SRM installation and configuration process for all of the servers in this deployment before proceeding.
12. Restart the services, and troubleshoot any service that does not show a status of "running."

```
manage-modules.cmd service restart all
manage-modules.cmd service status all
```

Configuring virus-scanning software

Running virus-scanning software on directories containing MySQL data and temporary tables can cause issues, both in terms of the performance of MySQL and the virus-scanning software misidentifying the contents of the files as containing spam.

After installing MySQL Server, it is recommended that you disable virus scanning on the directory used to store your MySQL table data (such as `C:\Program Files \APG\Databases\MySQL\Default\data`). In addition, by default, MySQL creates temporary files in the standard Windows temporary directory. To prevent scanning the temporary files, configure a separate temporary directory for MySQL temporary files and add this directory to the virus scanning exclusion list. To do this, add a configuration option for the tmpdir parameter to your my.ini configuration file.

CHAPTER 3

Uploading License Files

This chapter includes the following topics:

Uploading license files

Procedure

1. Download the license file from the license portal.
2. Open a browser and connect to the Storage Monitoring and Reporting installation page at the following URL:

   `http://<Frontend-hostname>:58080`

   The Storage Monitoring and Reporting installation page opens.
3. Provide the license file by dragging it onto the text box or clicking the text box and navigating to the file. If you provide multiple licenses, use the drop-down menu to specify which type of instance (VNX or VPLEX) you want to install.

   The installer analyzes the license file.
4. Click **Next**.
5. Enter a username and password for the admin user, confirm the password, and then click **Install**.

   The installation begins and a status bar shows the progress.
6. When the installation is complete, click **Restart application to complete the installation**.

   The system redirects you to **Discovery Center** to configure your devices.

CHAPTER 4

SolutionPack for EMC VNX

This chapter includes the following topics:

Overview

The SolutionPack for EMC VNX collects performance and capacity data from your Unity, VNX, and VNXe systems and displays the data in easy-to-use reports.

With this SolutionPack, you can unify your view of multiple Unity, VNX, and VNXe systems. Capacity reports, such as Raw Capacity Usage, Usable Capacity, and Usable Capacity by Pool, help you to improve the availability of business critical applications and services by ensuring that those applications have the storage resources they need to operate effectively. Performance reports provide key performance indicators for such fundamental resources as LUNs, Disks, and File Systems.

VNX prerequisites

The following sections apply when discovering VNX Block Only, VNX Unified/File, and VNX NAS Gateway/eNAS array types. These sections do not apply for Unity/VNXe2 array types. There are no discovery prerequisites for Unity/VNXe2 array types.

- Preparing your VNX for discovery and data collection
- Configuring simple authentication
- Unisphere security file authentication
- Configuring VNX arrays for file storage discovery

Preparing your VNX for discovery and data collection

Identify the information required to support resource discovery and data collection before installing the SolutionPack for EMC VNX and perform the necessary pre-configuration.

Storage Monitoring and Reporting uses Navisphere Secure CLI (NavisecCLI) to access the VNX arrays. NavisecCLI needs to be configured to the "low" security level to properly communicate with the arrays. In a vApp deployment, this is the default setting. However, for a binary install, be sure that you install NavisecCLI with the "low" security level.

EMC recommends matching Naviseccli versions with Block Operating Environment versions of VNX systems configured in the Collector. For information on compatible Block OE and Naviseccli versions, refer to the *VNX OE for Block Release Notes* and the *Unisphere Host Agent/CLI and Utilities Release Notes* on EMC Online Support.

For block and unified data collection, you must enable statistics logging on the array. To enable statistics logging, refer to Unisphere documentation.

To prevent Storage Monitoring and Reporting discovery issues after a VNX control station failover, ensure that the srmuser home directory exists on both the active and secondary control stations. When a Global or LDAP user is first created on a VNX, the user's home directory is created on the active control station. When the first failover to the secondary control station occurs, the VNX does not create the user's home directory on the secondary control station. Manually create the home directory on the secondary control station if needed.

Specifying a non-default NavisecCLI installation location

If NavisecCLI is installed in a non-default location, you must modify the location using the command line.

The default installation locations are:

- vApp – `/opt/Navisphere/bin/naviseccli`
- Windows binary – `C:\Program Files(x86)\EMC\Navisphere CLI\`
- Linux binary – `/opt/Navisphere/bin/naviseccli/`

Procedure

1. Open an SSH (Linux) or RDP (Windows) session to the Storage Monitoring and Reporting server.
2. Navigate to `<install_location>/APG/bin`.
3. Type the following command:

   Linux: `./manage-modules.sh update emc-vnx-collect emc-vnx`

   Windows: `manage-modules.cmd update emc-vnx-collect emc-vnx`
4. At each system prompt, accept the default with the following exceptions:
   - At the `Enter the step to modify, 'yes' to accept them, or 'no' to cancel the operation` prompt, type **`yes`**.
   - At the `Do you want to modify the module configuration?` prompt, type **`yes`**.
   - At the `Specify custom naviseccli path` prompt, type **`yes`**.
5. At the `Naviseccli Path` prompt, type the NavisecCLI path and hit Enter.
6. At the `Do you want to specify another Unity/VNX system?` prompt, type **`yes`**, and then keep accepting the defaults. This ensures that any devices that were previously provided are kept after modifying the NavisecCLI path.

Results

When you reach the end of the devices, the system restarts the collector with the updated NavisecCLI path.

```
./manage-modules.sh update emc-vnx-collect emc-vnx
Required dependencies, in processing order:
   [1]   java '8.0.92' v8.0.92
   [2]   topology-mapping-service 'Default' v1.4u1
   [3]   module-manager '1.10u1' v1.10u1
   [4]   license-manager 'Default' v5.6
   [5]   collector-manager 'emc-vnx' v5.8u1
   [6]   failover-filter 'emc-vnx' v5.2
   [7]   cross-referencing-filter 'emc-vnx' v1.6u1
   [8]   group-filter 'emc-vnx' v2.1u2
   [9]   variable-handling-filter 'emc-vnx' v1.15u1
  [10]   inline-calculation-filter 'emc-vnx' v6.3u1
  [11]   stream-collector 'emc-vnx' v1.3u1
  [12]   jdbc-drivers 'Default' v2.7u1
  [13]   script-engine 'Default' v1.4u1
  [14]   property-tagging-filter 'emc-vnx' v2.10u1
  [15] U emc-vnx-collect 'emc-vnx' v4.0 => v4.0
> 14 not modified, 1 to update
> 2.5 MB space required / 114.5 GB available
 ? Enter the step to modify, 'yes' to accept them, or 'no' to
cancel the operation [yes] > yes

Starting update of emc-vnx-collect emc-vnx from v4.0 to v4.0...
 * Gathering information...
 * Module found in '/opt/APG/Block/emc-vnx-collect/emc-vnx'.
```

```
 * It will now be updated using 'emc-vnx-collect-4.0.pkg'.
 * Unpacking files...
 * Updating files... 100%
 * 229 files have been updated.
 * Finalizing update...

 ? Do you want to modify the module configuration? (yes/no) [n] >
yes
 ? Activate the FailOver-Filter (yes/no) [y] >
 ? Hostname or IP address to send data to [localhost] >
 ? Network port to send data to [2020] >
 ? Tomcat hostname or IP address [localhost] >
 ? Configure custom Tomcat port (yes/no) [n] >
   [1] HTTP
   [2] HTTPS
 ? Tomcat communication protocol [1] >
 ? Username [ws-user] >
 ? Password [?????] >
 ? Frontend Web service instance name [APG-WS] >
 ? Topology Service hostname or IP address [localhost] >
 ? Web-Service gateway hostname or IP address [localhost] >
 ? Web-Service port number [48443] >
   [1] Basic
   [2] Certificate
 ? Authentication schema [2] >
 ? Event server hostname or IP address [localhost] >
 ? Event server port number [52001] >
 ? Configure Alert consolidation (yes/no) [n] >
 ? Specify custom naviseccli path (yes/no) [n] > yes
 ? Naviseccli Path > /opt/Navisphere/bin/naviseccli
 ? Do you want to specify another Unity/VNX system? (yes/no) [y] > y
   [1] VNX Block Only
   [2] VNX NAS Gateway/eNAS
   [3] VNX Unified/File
   [4] Unity/VNXe2
 ? VNX type [1] >
 ? Unique friendly name [FNM00083700047] >
 ? SP A IP [lglad053] >
 ? SP B IP [lglad054] >
 ? Use Naviseccli security file (yes/no) [n] >
   [1] LDAP
   [2] global
   [3] local
 ? Naviseccli User Scope [2] >
 ? Naviseccli Username [emc] >
 ? Naviseccli Password [?????] >
 ? More entries? (yes/no) [y] >
   [1] VNX Block Only
   [2] VNX NAS Gateway/eNAS
   [3] VNX Unified/File
   [4] Unity/VNXe2
 ? VNX type [4] >
 ? Unique friendly name [CF2EN154000003] >
 ? Management IP or hostname [10.247.28.164] >
 ? Username [admin] >
 ? Password [?????] >
 ? More entries? (yes/no) [n] >
 ? Use advanced settings (yes/no) [n] >

 * Updating service 'collector-manager emc-
vnx'...                    [ updated ]
 * Starting 'collector-manager emc-
vnx'...                                  [ OK ]
Update complete.
```

Configuring simple authentication

You can configure simple authentication with VNX arrays using the default Storage Monitoring and Reporting account.

In order to poll and collect performance statistics from a VNX array, administrator privileges are required for the user account used to access the arrays.

Note

The preferred method for secure polling and collection of data from VNX arrays is to configure authentication using a Unisphere security file. Refer to Unisphere security file authentication.

Procedure

1. Configure the default Storage Monitoring and Reporting account (apg) with administrator privileges to access the VNX array as described in the Unisphere documentation.
2. Validate access to the VNX array by running the following block command:
   naviseccli -h (host) -user *username* -password *password* -scope 0 getagent

Unisphere security file authentication

A Unisphere security file is the preferred method to provide secure polling and data collection from VNX arrays.

When you create a security file, the username you use to log in to the current host is automatically stored in the security file, or you can specify an alternative username for the security file in the `-AddUserSecurity` request using the optional `-user` switch. If you omit the `-user` switch, the security file uses your current username. You can also target the security file at a specific storage system using the `-ip` option.

You can store the security file on the Collector host and edit parser XML files to include this path which will provide the required authentication to access the arrays.

Note the following:

- By default, the security file is stored in your default home directory. With NavisecCLI, you can specify an alternative file path using the optional `-secfilepath` switch.
- Security files are generated exclusively for use by the user who creates them. By default, the EMC VNX collector manager runs under the accounts `apg` (for Linux) or `SYSTEM` (for Windows). In order to use a Navisphere CLI security file in this default configuration, the security file must be created using the above account(s). If the collector is configured to run as a different user (such as in the scenario described in the EMC White Paper *Running Windows Collector Services Using Least Privileges*, https://community.emc.com/docs/DOC-36060), the security file to be used by the collector must have also been created by that same user account.
- **Important:** For VNX collectors running on Windows, explicitly specifying the full security file path is required when configuring VNX discoveries, even if the security file resides in the default %USERPROFILE% directory.
- Once the security file exists, you can edit XML configuration files that are used to poll and collect data to specify the path to the security file on the Collector host. The security file handles authentication.

- For details on configuring a security file on a host, refer to the Unisphere documentation.

Configuring VNX arrays for file storage discovery

Learn how to configure VNX arrays for file storage discovery.

Procedure

1. Log into Control Station as the root user.
2. Open the `nas_mcd.cfg` configuration file in the `/nas/sys/` directory.
3. Enable the XML–API service by uncommenting the following entry:

```
daemon "XML API Server"
        executable      "/nas/sbin/start_xml_api_server"
        optional        yes
        canexit         yes
        autorestart     yes
        ioaccess        no
```

4. Type **`# service nas start`**, and press **Enter** to restart the XML-API service.
5. If you have multiple VNX arrays in your storage environment, repeat this procedure on each VNX array.

Adding and configuring devices in Discovery Center

Procedure

1. From **Discovery Center** > **Devices Management**, click **EMC VNX**.
2. Click **Add new device**.
3. If the **Server** field appears, select the server where the device will be dispatched.
4. If the **Instance** field appears, select the instance of the emc-vnx-collect where the device will be dispatched.
5. In **VNX type**, select **VNX Block Only**, **VNX NAS Gateway/eNAS**, **VNX Unified/File**, or **Unity/VNXe2**.

   If the following fields appear, enter the information specified:

   a. In **Unique friendly name for the VNX system**, type the name.

   b. In **SP A IP**, type the IP address of the SPA.

   c. In **SP B IP**, type the IP address of the SPB.

   d. In **Use Naviseccli security file**, select this checkbox if you are using the security file.

   e. In **Naviseccli User Scope**, select **LDAP**, **Global** or **Local**.

   f. In **Naviseccli Username** and **Naviseccli Password**, type the Naviseccli credentials for the block storage systems.

   g. In **Primary control station IP**, type the IP address of the primary control station.

   h. In **Secondary control station IP**, type the IP address of the secondary control station.

i. In **VNX File User Scope**, select **LDAP**, **Global**, or **Local**.

j. In **VNX File Username** and **VNX File Password**, type the credentials for the file storage system.

k. In **Management IP or hostname**, type the IP address for the Unity/VNXe2 system.

l. In **Username**, type the username for the Unity/VNXe2 system.

m. In **Password**, type the password for the Unity/VNXe2 system.

6. Click **Validate and Add** to validate the credentials.

Note

This button tests array connectivity and credentials using the default user apg (Linux) or SYSTEM (Windows). If the VNX collector-manager is configured to run under a custom user (not the default) and uses a Naviseccli security file that is configured for that user, the test results will show failures. However, these can safely be ignored if the underlying collector-manager user & security file are correctly configured.

7. Click **Ok**.
8. Click **Save**.

Changing VNX object credentials using Discovery Center

Using Discovery Center, you can export, modify, and then import VNX credentials.

Procedure

1. From **Centralized Management**, click **Discovery Center** > **Devices Management** > **EMC VNX**.
2. Click **Export** and save the .csv file.
3. Open the .csv file in a text editor, such as Notepad++.
4. In the file, identify the credentials that need to be changed.

   In the example below, the username and password for `test-user` has been identified.

```
Server,Instance,type,friendlyname,block.spa,block.spb,block.us
e_secfile,block.secfilepath,block.userscope,block.username,blo
ck.password,file.csprimary,file.cssecondary,file.username,file
.password,unity.management,unity.username,unity.password
'servername.emc.com','emc-
vnx','unified','FNM00130900273','lglad065','lglad066','false',
,'global','test-
user','{5D6FAF32A927B424BFD17D71D5F6C85AC37CE3232E9012FE490DE4
825098BCA753E17FDC23F4E60C53320DA7E9FCC4AA}','lglad064',,'nasa
dmin','{9039753E3695E8B7027D0B95749AF1620E2A392FB1224E6DF4A192
66F1F4859F6C6F7916124ACB801DB00BCADFBA6DCC}',,,
'servername.emc.com','emc-
vnx','block','FNM00083700047','lglad053','lglad054','false',,'
global','emc','{A921446A3F75CF9174C9365B8073E3F33732087BB8C269
4B8215AFA8051D970E4128A57E63342BE997C0BFE3C10F6468}',,,,,,,
```

5. Change the credentials in the .csv file.

In the example below, `test-user` has been changed to `test2` and the password has been changed to `password456`.

```
Server,Instance,type,friendlyname,block.spa,block.spb,block.us
e_secfile,block.secfilepath,block.userscope,block.username,blo
ck.password,file.csprimary,file.cssecondary,file.username,file
.password,unity.management,unity.username,unity.password
'servername.emc.com','emc-
vnx','unified','FNM00130900273','lglad065','lglad066','false',
,'global','test2','password456','lglad064',,'nasadmin','{90397
53E3695E8B7027D0B95749AF1620E2A392FB1224E6DF4A19266F1F4859F6C6
F7916124ACB801DB00BCADFBA6DCC}',,,
'servername.emc.com','emc-
vnx','block','FNM00083700047','lglad053','lglad054','false',,'
global','emc','{A921446A3F75CF9174C9365B8073E3F33732087BB8C269
4B8215AFA8051D970E4128A57E63342BE997C0BFE3C10F6468}',,,,,,,
```

6. Save the .csv file.
7. In **Discovery Center**, click **Import**.
8. Select the **Merge the devices with the existing ones?** checkbox.
9. Click **Browse** to find the .csv file with the new credentials.
10. Click **Ok**.

    A dialog appears indicating that the devices have been replaced (all of them will be refreshed, even if the credentials were only updated for one object).
11. Click **Continue**.

    The Discovery Center credentials page refreshes, displaying all contents in italics.
12. Click **Save** for the changes to take effect.

    This will restart the VNX collector instance(s) and update the credentials that are used.

Troubleshooting

Use this section to troubleshoot common errors.

Resolving collector communication errors

There may be cases where the collector runs into issues reaching the array. Some known examples are listed below.

When a VNX storage processor is not reachable via Navisphere Secure CLI (NavisecCLI) or when the NavisecCLI security file has not been properly configured, error messages like those shown below will appear in the collection logs.

```
SEVERE -- [2015-10-06 10:30:22 EDT] -- DataListener
$ValueFormatter::createValues(): No value found for key agent-spa-
memory, context VNX1 and properties {topopass=value,
friendlyname=APM00140634211, scopeflag=, spb=losat164.lss.emc.com,
spa=losat163.lss.emc.com, topouser=value, POLLING_COUNTER=0,
deviceid=1, command=/opt/Navisphere/bin/naviseccli,
topoport=localhost:48443, secfilepath=/tmp, userflag=,
sstype=Unified, password=,
```

```
cimauthorization=@{user}:@{password}:@{scope}, passwordflag=,
nopollflag=-nopoll, scope=, secfilepathflag=-secfilepath, user=}
```

```
SEVERE   -- [2015-10-06 11:50:22 EDT] --
AbstractStreamHandlerJob::prepareNextStep(): Error executing
handler XslStreamTransformer containing 1 sub handlers
com.watch4net.apg.ubertext.parsing.StreamHandlerException: Error
while transforming stream
        at
com.watch4net.apg.ubertext.parsing.transformer.XslStreamTransformer.
execute(XslStreamTransformer.java:58)
        at
com.watch4net.apg.ubertext.parsing.AbstractSimpleStreamHandler.handl
eExecution(AbstractSimpleStreamHandler.java:39)
        at
com.watch4net.apg.ubertext.parsing.concurrent.AbstractStreamHandlerJ
ob.prepareNextStep(AbstractStreamHandlerJob.java:180)
        at
com.watch4net.apg.ubertext.parsing.concurrent.SimpleStreamHandlerJob
.step(SimpleStreamHandlerJob.java:41)
        at com.watch4net.apg.concurrent.executor.AbstractJobExecutor
$SequentialJob.step(AbstractJobExecutor.java:419)
        at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor.executeJob
Runner(AbstractJobExecutor.java:122)
        at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor.access
$500(AbstractJobExecutor.java:22)
        at com.watch4net.apg.concurrent.executor.AbstractJobExecutor
$JobRunnerImpl.run(AbstractJobExecutor.java:274)
        at
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor
.java:1142)
        at java.util.concurrent.ThreadPoolExecutor
$Worker.run(ThreadPoolExecutor.java:617)
        at java.lang.Thread.run(Thread.java:745)
Caused by: net.sf.saxon.trans.XPathException: Error reported by XML
parser: Content is not allowed in prolog.
```

To resolve the communication issues shown above, follow the steps below.

Procedure

1. Using the collection logs, identify the VNX storage processor that is not able to communicate with the collector, as shown in the example error below:

   ```
   SEVERE -- [2015-10-06 10:30:22 EDT] -- DataListener
   $ValueFormatter::createValues(): No value found for key agent-
   spa-memory, context VNX1 and properties {topopass=value,
   friendlyname=APM00140634211, scopeflag=,
   spb=losat164.lss.emc.com, spa=losat163.lss.emc.com,
   topouser=value, POLLING_COUNTER=0, deviceid=1, command=/opt/
   Navisphere/bin/naviseccli, topoport=localhost:48443,
   secfilepath=/tmp, userflag=, sstype=Unified, password=,
   cimauthorization=@{user}:@{password}:@{scope}, passwordflag=,
   nopollflag=-nopoll, scope=, secfilepathflag=-secfilepath,
   user=}
   ```

   In this example, storage processor A on the array APM00140634211 cannot communicate with the collector.

2. Ensure the storage processor is reachable via NavisecCLI from the VNX collector host given the same credentials used in Storage Monitoring and Reporting.

3. Ensure that the NavisecCLI security file has been properly configured. For more information on configuring the security file, refer to Unisphere security file authentication.

Resolving creating stream errors

An error message, like the one shown below, will appear in the collection logs when the /opt/APG/Collecting/Stream-Collector/emc-vnx/./conf/output/vnxalerts-block-deviceid-1-laststarttime.xml files are deleted.

```
SEVERE - [2015-11-02 10:30:02 EST] -
AbstractStreamHandlerJob::prepareNextStep(): Error executing
handler FileReaderRetriever containing 1 sub handlers
 com.watch4net.apg.ubertext.parsing.StreamHandlerException: Error
while creating the stream for file /opt/APG/Collecting/Stream-
Collector/emc-vnx/./conf/output/vnxalerts-block-deviceid-1-
laststarttime.xml
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.new
FileToRead(FileReaderRetriever.java:340)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.exe
cute(FileReaderRetriever.java:189)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.exe
cute(FileReaderRetriever.java:46)
 at
com.watch4net.apg.ubertext.parsing.AbstractForkingStreamHandler.hand
leExecution(AbstractForkingStreamHandler.java:122)
 at
com.watch4net.apg.ubertext.parsing.concurrent.AbstractStreamHandlerJ
ob.prepareNextStep(AbstractStreamHandlerJob.java:180)
 at
com.watch4net.apg.ubertext.parsing.concurrent.ForkingStreamHandlerJo
b.step(ForkingStreamHandlerJob.java:46)
 at
com.watch4net.apg.concurrent.executor.DefaultScheduledJobExecutor
$ScheduledJob.step(DefaultScheduledJobExecutor.java:249)
 at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor.executeJob
Runner(AbstractJobExecutor.java:122)
 at com.watch4net.apg.concurrent.executor.AbstractJobExecutor.access
$500(AbstractJobExecutor.java:22)
 at com.watch4net.apg.concurrent.executor.AbstractJobExecutor
$JobRunnerImpl.run(AbstractJobExecutor.java:274)
 at
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor
.java:1142)
 at java.util.concurrent.ThreadPoolExecutor
$Worker.run(ThreadPoolExecutor.java:617)
 at java.lang.Thread.run(Thread.java:745)
 Caused by: java.io.FileNotFoundException: /opt/APG/Collecting/
Stream-Collector/emc-vnx/./conf/output/vnxalerts-block-deviceid-1-
laststarttime.xml (No such file or directory)
 at java.io.FileInputStream.open0(Native Method)
 at java.io.FileInputStream.open(FileInputStream.java:195)
 at java.io.FileInputStream.<init>(FileInputStream.java:138)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.new
FileToRead(FileReaderRetriever.java:336)
 ... 12 more
```

To resolve this issue, follow the steps below.

Procedure

1. From **Centralized Management**, click **SolutionPacks** > **Storage** > **EMC VNX**.
2. Click the pencil icon for the **Data collection** component to reconfigure the SolutionPack.

   The missing files are recreated.

Limitations

- VNX Free Raw Disk Capacity values are not the same as EMC Unisphere Free Raw Capacity values. Unisphere Free Raw Capacity counts both internal operation space (vault drives) and the space available for user LUNs. Free Raw Disk Capacity only counts the space available for user LUNs.
- **Hot Spare** values are incorrect for VNX arrays running Operating Environment for Block / FLARE 05.33.x. In that version, the VNX series supports a new hot spare policy where any unbound disk is available for use as a hot spare. Therefore, disks are not specifically marked as hot spares, but rather as unbound disks. As a result, hot spare disks are incorrectly counted as unconfigured capacity.
- VNX Statistics Logging will stop when VNX Performance Logging stops if Performance Logging was enabled before Statistics Logging was enabled. To prevent this from happening, manually enable Statistics Logging via Unisphere or NaviCLI (using the `setstats -on` command) before enabling Performance Logging (which is optional). In this way, even if the optional Performance Logging stops, performance metrics will continue to be collected.
- The following error message appears in the logs during the first couple polling cycles when an array is discovered; after that the message will stop:

```
SEVERE   -- [2016-01-28 10:44:39 EST] --
FileDownloadingTask::run():
com.watch4net.apg.ssh.api.exception.SSHException: Remote
directory './emc-srm/server_2/3600' does not exist.
com.watch4net.apg.file.retriever.ClientException:
com.watch4net.apg.ssh.api.exception.SSHException: Remote
directory './emc-srm/server_2/3600' does not exist.
```

- The discovery of VNX/Unity/VNXe arrays using an IPv6 address in Discovery Center is not supported. Use the hostname which resolves to the respective IPv6 address when entering the details for SPA, SPB and Control Station (for VNX) or for Management Host (for Unity/VNXe2).
- The following message appears in the logs when the SolutionPack for VNX collector-manager is first started. This problem is resolved when a device is added for discovery and the collector-manager is restarted.

```
WARNING - [2016-04-10 11:26:24 EDT] - SocketConnector::init():
Can't connect socket to localhost:52001
 java.net.ConnectException: Connection refused
```

- If the "Current Owner" of a LUN on a Unity or VNXe2 array changes, the 'memberof' property will display multiple values for a while until the collection has time to normalize things. For Unity, that means that for approximately one hour (by default, or up to four hours if 60 mins topology polling period is selected), the reports will show multiple values for the 'memberof' property. For VNXe2, that

means that until the LUN metrics are marked inactive (approximately 24 hours), the reports will show multiple values for the 'memberof' property.

- It is possible for existing VNX array LUNs to appear in the **Inactive Devices & Components** report. This occurs because the `memberof` property is part of the LUN variable id. If a LUN trespasses between storage processors, the old instance of the metric will be tagged with an inactive `vstatus` property.
- The following warning might appear in the logs when the Primary control station of a VNX Unified or NAS Gateway is not reachable or does not respond to XML API requests:

```
WARNING  -- [2016-06-06 09:08:38 EDT] --
HttpRequestGroup::executeRequest(): Error running command
https://@{cssecondary}/Login?user
java.lang.IllegalArgumentException: Host name may not be
null....
```

This can occur when the VNX Unified or NAS Gateway has only one control station, and the Secondary control station IP field is blank.

CHAPTER 5

SolutionPack for EMC VPLEX

This chapter includes the following topics:

Overview

The SolutionPack for EMC VPLEX allows you to visualize and report on performance and capacity data from your VPLEX systems.

With this SolutionPack, you can unify your view of multiple VPLEX systems, including physical storage to virtual storage relationships. Capacity reports, such as Thick, Thin, Allocated and Not Allocated, help you to improve the availability of business critical applications and services by ensuring that those applications have the storage resources they need to operate effectively.

Adding and configuring devices in Discovery Center

Before you begin

- While adding a new device, ensure that cluster 1 IP and serial number are not interchanged with the cluster 2 IP and Serial Number.

Procedure

1. Click **Discovery Center** > **Devices Management**.
2. Click **VPLEX**.
3. Click **Add new device**.
4. In the **VPLEX** section, provide the cluster host and authentication details for your VPLEX system.

   The default username for the VPLEX is `service` and the default password is `Mi@Dim7T`. For the ViPR SRM username to have all of the required permissions on the array, you must use `service` as the username. The password can be changed from the default.

   It is important to enter the cluster information correctly, clusters are mapped to their correct number. Interchanging cluster IPs and SN results in a failure to collect performance data.

   Be sure to select the correct VPLEX type while adding the device. If you are adding a VPLEX Metro or VPLEX Geo, select the **Geo/Metro** VPLEX type from the drop-down and enter both VPLEX cluster details. If you are adding a VPLEX Local, select the **Local** VPLEX type from the drop-down and enter the VPLEX cluster details. Do not add a Geo or Metro VPLEX System as two separate Local VPLEX Systems.
5. Click **Validate and Add** to validate the credentials.
6. Click **Ok**.
7. Click **Save**.

   It will take approximately take three hours for data to start appearing on reports.

After you finish

Note

Threshold based alerts are disabled by default. To manually enable threshold based alerts, go to **Administration** > **Modules** > **Alerting** > **Alert Definitions** > **EMC VPLEX Alert Definitions**. (SNMP based alerts are enabled by default.)

Troubleshooting performance data collection issues

Ensure that on each VPLEX cluster, VPLEX Perpetual monitors are not stopped and are logging director and virtual volume performance data. To do this, login to VPLEX and look for the Perpetual Monitor log files located at `/var/log/VPlex/cli/director*PERPETUAL*.log`. There are separate perpetual monitor log files for VPLEX Directors and VPLEX virtual volumes. And for each type, there is one log file per director. These log files are used to collect performance data. Ensure that the last modified time stamp for all such log files is not older than a few minutes.

In case the perpetual monitor log files are old, it means that the perpetual monitors have stopped and you may not this data be collected. VPLEX KB articles have more information on how to resolve this issue.

Configure VPLEX SNMP

Configure your VPLEX server to send SNMP traps to Storage Monitoring and Reporting on port 2041.

For more information about configuring SNMP on VPLEX, refer to the *EMC VPLEX Administration Guide*.

Procedure

1. Log into the VPLEX CLI.
2. From the `VPlexcli:/>` prompt, enter: **`cd notifications/call-home/snmp-traps/`**
3. Create a trap using the command: **`create <trap-name>`**

   Where <*trap-name*> is any string that you want to use.
4. cd to <*trap-name*>.
5. Configure the trap to send notifications to Storage Monitoring and Reporting using the command: **`set remote-host <IP address>`**

   Where <*IP address*> is the IP address of the server receiving the traps. For example, on a four VM deployment, this is the IP address of the Primary Backend.
6. Configure the trap to send data to port 2041 using the command: **`set remote-port 2041`**
7. Start sending notifications by using the command: **`set started true`**

Limitations

Only encapsulated virtual volumes are supported. LVM virtual volumes are not supported.

CHAPTER 6

Logging into the User Interface

This chapter includes the following topics:

Logging in to the user interface

Log in to the user interface to view, schedule, and export reports.

Procedure

1. Open a browser and type the following URL:

   `http://<Frontend-hostname>:58080/APG`

2. Type the login credentials that you provided during the License Upload step of the installation.
3. Click **Sign In**.

Note

You are automatically logged off after four hours.