Embedded Management on PowerMax and VMAX All Flash

Embedded Management (eManagement) with Unisphere for PowerMax

Dell EMC Engineering
May 2018
## Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2018</td>
<td>Initial release</td>
</tr>
</tbody>
</table>

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA [4/20/2018] [Technical White Paper] [H16856]

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
# Table of contents

Revisions ................................................................................................................................. 2

Executive summary .................................................................................................................. 4

1 PowerMax Hypervisor ........................................................................................................ 5
   1.1 Hypervisor CPU Core Allocation – Multi-Core Emulation ........................................ 5
   1.2 Hypervisor Memory Allocation .................................................................................. 6
   1.3 Hypervisor Storage Allocation – Cut-Through Device (CTD) ..................................... 7
   1.4 Hypervisor Network Connectivity ............................................................................. 7

2 Embedded Management ..................................................................................................... 8
   2.1 eManagement High Availability ............................................................................. 10
   2.2 Unisphere Authentication Security ........................................................................... 12

3 vApp Manager .................................................................................................................... 14
   3.1 Exporting Log and Performance Files ..................................................................... 15
   3.2 Configuration Changes ............................................................................................. 17
   3.3 vApp Manager Authentication Security ................................................................... 19
   3.4 Certificates ................................................................................................................ 20

4 Solution Enabler Client / Server Configuration ............................................................... 22
   4.1 Configuring the Server ............................................................................................. 22
   4.2 Configuring the Client ............................................................................................. 24

5 Conclusion .......................................................................................................................... 26

A Appendix A: References ..................................................................................................... 27
Executive summary

**Dell EMC PowerMax** family and VMAX® All Flash customers can take advantage of simplified array management using embedded Unisphere for PowerMax. Unisphere is an intuitive HTML5 web-based management interface that allows IT managers to maximize productivity by dramatically reducing the time required to provision, manage, and monitor storage assets.

Embedded Unisphere enables customers to simplify management, reduce cost, and increase availability by running PowerMax and VMAX All Flash management software directly on the array. Embedded management is configured in the factory to ensure minimal setup time on site. The feature runs in a container within the PowerMaxOS Hypervisor, eliminating the need for a customer to allocate their own equipment to manage their arrays. Aside from Unisphere, other key elements of the eManagement data service include Solutions Enabler, Database Storage Analyzer, and SMI-S management software.

Unisphere for PowerMax delivers the simplification, flexibility, and automation that are key requirements to accelerate the transformation to the all flash data center. For customers who frequently build up and tear down storage configurations, Unisphere for PowerMax makes reconfiguring the array even easier by reducing the number of steps required to delete and repurpose volumes. Using Unisphere for PowerMax, a customer can set up a multi-site SRDF configuration in a matter of minutes.
1 **PowerMax Hypervisor**

PowerMaxOS 5978 runs on the Dynamic Virtual Matrix leveraging its scale out flexibility of cores, cache, and host interfaces. The embedded storage hypervisor reduces external hardware and networking requirements, delivers high levels of availability, and dramatically reduces latency. Hypervisor upgrades are performed non-disruptively.

Within the PowerMax Hypervisor, virtual machines (VMs) provide the host platform that includes CPU processing, memory, network interface card (NIC), ports, data storage by using a Cut-Through Device (CTD), and external network through the Management Module Control Station (MMCS). VMs run within the front end FA emulation.

Figure 1 shows the primary components of the PowerMax and Hypervisor.

![Figure 1](image)

**Hypervisor Concepts – Virtual Machines**

1.1 **Hypervisor CPU Core Allocation – Multi-Core Emulation**

Using the Multi-Core emulation capability in PowerMax and VMAX All Flash, the CPU processing is provided using CPU cores from the FA emulation. The cores are pooled for front-end, back-end, and for PowerMaxOS functions as shown in Figure 2. All of the CPU cores on the director can work on I/O from all of the ports. This helps ensure the directors’ ports are always balanced.
1.2 Hypervisor Memory Allocation

Memory is allocated to the hypervisor from the director cache during the initial setup as shown in Figure 3. This memory is then allocated to each Virtual Machine (VM) on that director for the purpose of embedded applications. The amount of memory allocated to a VM is dependent on the type of application, for example Embedded Management.
1.3 Hypervisor Storage Allocation – Cut-Through Device (CTD)

Data storage for both the boot and application data is provided using a Cut-Through Device (CTD) as shown in Figure 4, which acts like an HBA that accesses LUNs in the PowerMax and VMAX All Flash. The CTD has two components to enable access to the LUNs through an FA port. The first is the CTD Server thread. This runs on the FA emulation and communicates with the CTD Client in the embedded operating system. The second is the CTD Client Driver. The CTD Client Driver is embedded in the host operating system and communicates with the CTD server running on the FA emulation. An operating system running in a VM must have the CTD client driver installed to access the LUNs.

Embedded application ports are virtual ports specifically provided for use by the VMs that contain the applications, such as Embedded NAS. They are addressed as ports 32-63 per director FA emulation. The virtual ports are provided to avoid contention with physical connectivity. As with physical ports, LUNs can be provisioned to the virtual ports.

1.4 Hypervisor Network Connectivity

Network connectivity for the VMs is provided by a virtual NIC (vNIC). The vNIC is connected to the internal network providing communication to PowerMaxOS and other VM instances. The VM management external network connectivity is provided through a PowerMaxOS component called the network address translation (NAT) Gateway which is part of the Infrastructure Manager (IM) emulation. The NAT Gateway provides translation services between external and internal IP addresses and utilizes a separate network connection on each of the two Management Module Control Stations (MMCS). A PowerMax or VMAX All Flash array with eManagement and ESRS connectivity would then require a total of 4 physical network connections and 4 IP addresses. Additional IP addresses would be required if Embedded NAS is also configured.
Embedded Management

Unisphere for PowerMax is a HTML5 web-based application that allows you to configure and manage PowerMax and VMAX All Flash storage systems. HTML5 Unisphere provides a number of advantages:

- Improved security
- Reduced application response times
- Modern user interface “look and feel”
- Aligns with other Dell EMC products
- Manage user accounts and roles
- Perform configuration operations (create thin volumes, mask volumes, set storage attributes, set volume attributes, and set port flags)
- Perform and monitor replication and backup operations:
  - TimeFinder® SnapVX
  - TimeFinder VP Snap
  - TimeFinder(Clone
  - TimeFinder/Mirror
  - Symmetrix Remote Data Facility (SRDF®)
  - Open Replicator for Symmetrix (ORS)
  - ProtectPoint™
- Manage advanced storage features, such as:
  - Service levels
  - Workload planning
  - Enhanced Virtual LUN Technology
  - Auto-provisioning Groups
  - Virtual Provisioning
  - Non-disruptive migration (NDM)
  - Embedded NAS (eNAS)
  - Fully Automated Storage Tiering (FAST)™
  - FAST.X
- Monitor alerts, including the ability to configure external alert notifications
- Monitor storage system performance data:
  - Monitor performance and capacity over time
  - Drill-down through data to investigate issues
  - View graphs detailing system performance
  - Set performance thresholds and alerts
  - View high frequency metrics in real time
  - Perform root cause analysis
  - View storage system heatmaps
  - Execute scheduled and ongoing reports (queries), and export that data to a file
  - Use predefined dashboards for many of the system components
  - Customize your own dashboard templates
  - Execute scheduled export of performance dashboards
- Monitor and troubleshoot database performance issues using Database Storage Analyzer
Unisphere has traditionally been installed on a dedicated Windows or Linux server, or deployed as a Virtual Appliance (vAPP). This approach enables the customer to manage multiple systems from a single Unisphere instance. With the release of HYPERMAX OS 5977.691.684 and later it is possible to run Unisphere as an appliance directly on the VMAX All Flash controllers within the native Hypervisor. This option is called Embedded Management (eManagement) and removes the need for an external management host to control and manage PowerMax and VMAX All Flash arrays.

eManagement is installed as two virtual machines for redundancy and high availability. The VMs are distributed based on the mirrored pair architecture of PowerMax and VMAX All Flash arrays to evenly consume resources for both performance and capacity.

eManagement uses the following resources:

- 8 Shared Logical CPU Cores (4 per eManagement, shared with the FA emulation)
- 818GB Total Storage Space (Boot, Persistent, and Shared)
- 2 IP addresses
- The total memory resources vary depending on the model as depicted in Table 1.

Table 1  Unisphere Resource Comparison

<table>
<thead>
<tr>
<th>Components</th>
<th>VMAX All Flash</th>
<th>PowerMax</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMAX 250F/FX</td>
<td>VMAX 450F/FX</td>
</tr>
<tr>
<td>Memory (GB)</td>
<td>24</td>
<td>32</td>
</tr>
</tbody>
</table>

To launch Unisphere, type either of the following URLs in a web browser:

- https://<eManagement_IP>:8443
- https://<eManagement_host_name>:8443

At the login window, as shown in Figure 5, type the Unisphere Initial Setup User username and password, and click Login.
The default username for the Unisphere Initial Setup User is **smc** and the default password is **smc**.

**Note:** For more information on using Unisphere, refer to the Unisphere online help.

### 2.1 eManagement High Availability

eManagement high availability is achieved with an Active-Standby model for the following embedded services:

- Unisphere
- SMIS

The following services run as local services on each of the eManagement VMs:

- vApp Manager
- Solutions Enabler Daemons
  - Base
  - GNS
  - Watchdog
  - STP
  - SYMAP Server
  - Witness Manager
Unisphere will respond to client requests on both external IP addresses under all normal operating conditions, including after a failover has occurred. Figure 6 shows how the network connections for the Active-Standby services failover from the active to the standby eManagement VMs.

When the active Unisphere instance becomes unavailable causing a failover, users of the Unisphere GUI will be subject to errors in outstanding activities and wizard sequences will be disrupted. The user will be logged out during a failover. REST client programs experience errors during the failure and failover, but may be written to recover from these errors automatically.

On the standby eManagement VM, the SMAS and SMAS DB Daemons will show as not running. This is a normal state and can be viewed in the vApp Manager Manage Daemons pane as shown in Figure 7.
2.2 Unisphere Authentication Security

Embedded Unisphere supports the following types of authentication:

- **LDAP**
  - Users login with their LDAP-SSL username and password (if they have a user account stored on a LDAP-SSL server).
  - To use this method: a Unisphere Administrator or SecurityAdmin sets up LDAP-SSL authentication in Unisphere. The Unisphere Online Help contains instructions on performing these tasks.

- **Local Unisphere users**
  - Users login with their Unisphere username and password (if they have a local Unisphere user account).
  - To use this method: a Unisphere Initial Setup User, Administrator, or SecurityAdmin creates a local Unisphere user account for the user. Local user accounts are stored locally on the SMAS server host and work in much the same way as the other methods to validate user credentials. The Unisphere Online Help contains instructions on performing these tasks.

- **X.509 certificate-based user authentication**
  - Certificate-based user authentication using X.509 certificates is supported on eManagement. A certificate issued by a trusted public third-party certificate authority (CA) can be used to authenticate trusted identity when using the Unisphere web client or REST API interfaces. The use of digital identity smartcards such as Common Access Card (CAC) and Personal Identity Verification (PIV) as part of a multi-factor authentication process is also supported.
  - Certificate-based user authentication can be enabled in the vApp Manager Import Certificate Wizard and after being confirmed, the choice becomes irreversible. The CA certificates must be imported before certificate-based user authentication can be used. The vApp Manager Online Help contains instructions on performing these tasks.

To view the authentication authorities as shown in Figure 8, open the **Settings** panel, select **Users and Groups > Authentication**.
Figure 8  Unisphere Authentication

Note: Windows OS/AD only applies to Unisphere installed on Windows hosts.

The *Dell EMC PowerMax Security Configuration Guide* provides additional details about authentication, authorization and other issues related to security.
vApp Manager

Each eManagement container also includes a HTML5 Virtual Appliance (vApp) Manager that provides the ability to configure your storage environment. Using the vApp Manager web interface, you can perform the following tasks:

- Launch Unisphere
- Monitor the application status
- Start and stop selected daemons
- Download persistent data
- Configure the nethost file (required for client access)
- Discover storage systems
- Modify options and daemon options
- Add host-based license keys
- Run a limited set of Solutions Enabler CLI commands
- Load VMAX-based and PowerMax-based eLicenses
- Configure LDAP
- Download SYMAPI debug logs
- Import CA signed certificate for web browser
- Import custom certificate for storsrvd daemon
- Check disk usage
- Clear temporary files
- Restart appliance
- Configure symavoid entries
- Manage users
- Reset hostname
- Update /etc/hosts file

The vApp Manager can be accessed by going to either of the following URLs in a web browser:

- https://<eManagement_IP>:5480
- https://<eManagement_host_name>:5480

When the user logs in for the first time the default login is used with username and password as seconfig.

Note: The default password needs to be changed for each of the two vApp Manager instances.
The vApp Manager dashboard in Figure 9 provides details on eManagement version, network information, authentication authority, and disc usage. This white paper covers common tasks. For detailed information on using the vApp Manager refer to the Dell EMC vApp Manager for eManagement Online Help.

3.1 Exporting Log and Performance Files

The following log and performance files are available in the vApp Manager Download menu shown in Figure 10:

- Daemon Logs
- Persistent Logs
- DELL EMC Grab Files
- vApp Manager Logs
- Export log and data files
- Clear Temporary Files
To export specific files, select **Export log and data files**. This will open an option window to select the product log and data file you wish to download as seen in Figure 11. After selecting the product, Figure 12 shows how files can be filtered out and selected based on date and file name.
3.2 Configuration Changes

eManagement IP address, host name, DNS servers, and NTP configuration is set up at the time of PowerMax and VMAX All Flash installation. Using the vApp Manager for eManagement, those settings can be changed without customer service intervention.

To change the host or domain name, from vApp Manager, navigate to the Host Configuration pane as seen in Figure 13 by selecting Configure > Host. Then select Change Host Name or Change Domain Name.

From the Host Configuration pane, the eManagement hosts file can be edited to add hosts not part of the configured DNS.
Figure 13  Host Configuration

To view or change the IP configuration of eManagement, navigate to IP Configuration and IPv4 or IPv6. In Figure 14 there are options to Get Config and show the current values, change the current values by typing the new value in the text box and click Set Config or clearing the text box with Reset Config.

Note: The default internal restricted IP address ranges that should not be used are: 172.16.0.0/16; 172.17.0.0/16; 172.18.0.0/16. Please see the PowerMax Site Planning Guide for additional information.
3.3 vApp Manager Authentication Security

The vApp Manager provides two types of user authentication:

- Local directory authentication (username and password)
- LDAP (Lightweight Directory Access Protocol) authentication

LDAP allows for distributed directory information services over a network of hosts. A client must provide a set of parameters to configure LDAP, which then allows connection to the LDAP server, and secures communication between hosts on the network.

To configure LDAP, navigate to the LDAP configuration wizard as seen in Figure 15 by selecting Configure > LDAP and completing the required fields.
Managing local and LDAP authenticated users is performed by selecting Manage > Accounts.

3.4 Certificates

A certificate is an electronic document that is used to identify a server, a company, or some other entity, and associates that identity with a public key. At installation, the installer generates and installs the self-signed server certificate used for HTTPS transport-level security. Users can replace this certificate with the one issued by a trusted third-party using the vApp Manager.

A certification authority (CA) is a third-party entity that validates identities and issues certificates. The certificate that the CA issues binds a particular public key to the name of the entity that the certificate identifies (such as the name of a server or device). Only the public key that the certificate certifies works with the corresponding private key that is possessed by the entity that the certificate identifies. Certificates help prevent the use of fake public keys for impersonation.

A Certificate Signing Request (CSR) is a message that an applicant generates and sends to a CA in order to apply for a digital identity certificate. Most third-party CA companies require a CSR before the company will create a digital certificate. When a CSR is generated, a key pair is also created. The applicant sending the CSR keeps the private key and asks the CA to sign the certificate. This method is more secure, because the private key stays with the applicant.

The vApp Manager provides a wizard that walks through the process of obtaining a CSR and importing CA certificates for the appliance and for Unisphere.

The process for obtaining a CA certificate is:

1. Create a self-signed certificate
2. Create a CSR
3. Submit CSR
4. Import CA-signed certificate
5. Verify CA-signed certificate

To replace the certificate for either the vApp Manager, Unisphere Server, or Solutions Enabler navigate to the Import Certificate Wizard as seen in Figure 16 by selecting Manage > Certificates. Select the appropriate application to import the customer SSL certificate.

![Import Certificate Wizard](image)

Figure 16 Import Certificate Wizard

To enable X.509 Certificate-based User Authentication, select the Unisphere Server Authentication wizard.

**Note:** For more detailed steps on importing certificates, refer to the vApp Manager online help.
4 Solution Enabler Client / Server Configuration

Solutions Enabler provides hosts with the Symmetrix Command Line Interface (SYMCLI). The SYMCLI is a comprehensive command set for managing your environment. SYMCLI commands can be invoked on the command line or within scripts. These commands can be used to monitor device configuration and status and perform control operations on devices and data objects within your storage environment. eManagement doesn't provide a direct command line interface for administrators that want to be able to utilize the feature rich command line of Solutions Enabler, it does however provide a client server mechanism by which this can be achieved.

4.1 Configuring the Server

The eManagement server must be configured to accept client server connections. This is done by configuring the storsrvd daemon process. Access for administering the system is via vApp Manager for eManagement.

The eManagement vApp is configured as a server, which runs the storsrvd daemon and provides the SYMAPI server access. Only hosts that are configured through the nethost settings can connect as clients to run Solutions Enabler SYMCLI commands. Providing your eManagement server was configured with DNS servers that are able to resolve the fully qualified domain name (FQDN) of your host that will run Solutions Enabler, you can enter the FQDN of your server and an authorized user into the nethosts file. The IP address of the client can be entered if DNS is not available. If multiple users are to be specified for a server they must be entered one at a time. Wild cards are also accepted on the user field however this is not advisable for obvious security concerns.

The nethosts file configuration menu is accessed from the Configure > Solutions Enabler tab as shown in Figure 17.
Figure 17  Nethosts Configuration

Once all of the entries for client hosts and users configured, the settings will be visible in the View Nethosts pane. If a mistake has been made or a decision has been made to revoke client server access for a host, an option to remove the hostname and user is next to the entry. Simply select the trashcan icon to delete.

The Solutions Enabler Base Configuration has to be configured to allow the Client/Server communication. This is accessed from Configuration > Solutions Enabler Base Configuration tab. At the bottom of the options is Use Access ID, set this value to ANY as seen in Figure 18.
4.2 Configuring the Client

After the nethosts file has been setup on the server, the next step is to configure the client for access to the server. Solutions Enabler needs to be installed on the client host. Download the appropriate version from https://support.emc.com and follow the install instructions. With Solutions Enabler installed the netcfg file needs to be configured to point to the server which will be the eManagment server that has just been configured.

The netcfg file is located in C:\Program Files\EMC\SYMAP\config on windows systems and /var/symapi/config if the host is linux or most variants of unix. If the default locations were changed on the install of Solutions Enabler then this file may be located elsewhere.

Open the netcfg file in a text editor and scroll to the end. The default entries are similar to those shown in Figure 19.

```
# This is a sample config for Ordered Pair of entries. SYMCLI will attempt
# to use the first one, and on failure use the second.

# SYMAP_ORDERED  Ordered    TCPIP  node001  WWW.XXX.YYY.ZZZ  2707  SECURE
# SYMAP_ORDERED  Ordered    TCPIP  node002  WWW.XXX.YYY.AAA  2707  SECURE
```

Figure 19  Default netcfg
The default entries can be used by removing the # at the start and end of the lines and enter the IP address for the two external (NAT) IP for your eManagement servers. The Ordered entries try to connect to the first and if that fails the client will connect to the second as per the High Availability setup. In the example shown in Figure 20, the netcnfg file has been modified to add a custom connect string “eManagement”. Using this method it’s possible to have multiple entries and choose to manage one of many systems.

```
# This is a sample config for Ordered Pair of entries. SYMCLI will attempt to use the first one, and on failure use the second.
#
# SYMAPI_ORDERED Ordered TCPIP node001 WWW.XXX.YYY.ZZZ 2707  SECURE #
# SYMAPI_ORDERED Ordered TCPIP node002 WWW.XXX.YYY.AAA 2707  SECURE #

eManagement Ordered TCPIP eManagement_host1 10.10.10.10 2707  SECURE
eManagement Ordered TCPIP eManagement_host2 10.10.10.11 2707  SECURE
```

Figure 20  Example Netcnfg File

Now that the netcnfg file has been configured, all that remains is to set an environment variable in your command prompt to connect the client to the server and verify the connection. Figure 21 below shows the SYMCLI_CONNECT variable set on a Windows system to match the entry in the netcnfg file. On Linux/Unix hosts, the export command is substituted for set.

```
C:\>set SYMCLI_CONNECT=eManagement

C:\>symcli -def

Symmetrix Command Line Interface (SYMCLI) Version V9.0.0.0 (Edit Level: 2500)
Built with SYMAPI Version V9.0.0.0 (Edit Level: 2500)

Current settings of the SYMCLI environment variables:
   SYMCLI_CONNECT :eManagement
```

Figure 21  SYMCLI environmental variable
5 Conclusion

Embedded Unisphere for PowerMax enables customers to simplify management, reduce cost, and increase availability by running PowerMax and VMAX All Flash management software directly on the array.

Unisphere for PowerMax is an intuitive HTML5 based management interface that allows IT managers to maximize productivity by dramatically reducing the time required to provision, manage, and monitor storage assets. Unisphere for PowerMax delivers the simplification, flexibility, and automation that are key requirements to accelerate the transformation to the all flash data center.
Appendix A: References

Dell EMC Unisphere for PowerMax Online Help
Dell EMC vApp Manager for eManagement Online Help
Dell EMC PowerMax Family Security Configuration Guide
Dell EMC PowerMax Family Site Planning Guide