Vormetric Data Security Manager

Release Notes for Vormetric Data Security Manager (DSM)

Release 6, Version 6.0.1

Document Version History

The following table describes the documentation changes made for each document version.

Table 1: Documentation Changesk

Documentation Version	Date	Changes
version 1	05/26/2017	6.0.1 G.A release.
version 2	02/21/2018	Separated VTE and VAE/VKM compatibility tables for clarity

New Features & Enhancements

The DSM v6.0.1 release introduces the following new features:

- **Bonded NICs**—support for aggregating the two NICs available on the DSM into a a single logical interface to provide load-balancing and/or fault tolerance. Refer to the *DSM Installation & Configuration Guide* for details.
- **Re-Sign updates to host settings**—changes to host settings are no longer automatically signed. Prior to this release, any changes to host settings that were pushed to the host from the DSM would result in a regeneration of the signatures. As of v6.0.1, changes to host settings will not generate an update of the signature without the explicit permission of the DSM Administrator. Refer to the *DSM Administrators Guide* for details.
- **DSM and Agent communication**—a new concise initialization method has been added that reduces the load on the DSM and the network when the agents are re-initialized. This means, once policies have been pushed to the hosts when they are first configured, any subsequent re-initialization of the agents is significantly faster.

Enhancements have been made to the following features:

- **High Availability**—The DSM UI displays high availability status on the Dashboard, administrators can now see the synchronization status of failover nodes as soon as they log on, and can take immediate action if there is a problem. Administrators can also log on to the failover node to view when it was last synchronized with the primary node. The high availability page on the failover now displays the exact time and date of the last synchronization with the primary node.
- **KMIP**—This feature has been enhanced to support:
    - KMIP protocol versions 1.0, 1.1, 1.2, 1.3, and 1.4
    - IPv6 for KMIP
    - KMIP Client requests from both primary and failover nodes
    - The certificate chain can now be retrieved from the KMIP server.
- **DSM RESTful API**—a new endpoint has been added to return the DSM server role (primary or failover).
- **Security updates**—This release of the DSM contains several security updates.

Resolved Issues

- **(SRV-15904) - Unable to add a host after deleting it from the GUI**

  A host with one-way communication, was deleted via the DSM Management Console and the host was removed from the UI. An attempt to add that same host to the DSM failed with the message that the host was still in use, indicating that the host had not actually been deleted.

  This issue has been resolved, and in the event that the host is not deleted when it receives the next status push from the DSM, it can be deleted as follows:

  On the DSM Management Console *Host* page, select the host to be deleted. The **Delete Pending** column indicates the host as marked for deletion with a check mark.

  a: Click on the host name to view the *Edit Host* page.

  b: Clear the **Registration Allowed** checkbox, click **Ok** to return to the *Host* page.

  c: Select the host again and click **Delete**. The host is removed from the DSM.

- **(SRV-15494) - Automatic Backup to a Windows share failed if the Windows account password was more than 30 characters long**

  A user with a Windows user account that had a password more than 30 characters in length, created a share location. A DSM automatic backup was to be saved to this location, but failed due a password length restriction attribute on the DSM.

  This issue has now been resolved and the DSM supports passwords up to 128 characters in length.

- **(SRV-16471) - Running the ‘`gencert`’ command on a failover node to obtain primary node certificate, fails**

  A user ran the `gencert` command on a failover node to obtain the primary node certificate after entering the wrong login credentials, the command fails with an error message stating that it failed to make an SSL connection to the primary node.

  This issue has been resolved and running the `gencert` command on the failover is successful.

- **(SRV-17996) - Unable to delete a domain after changing the license type**.

  This issue is now resolved and changing the license type does not affect the ability to delete a domain—a domain can still be deleted successfully.

- **(SRV-16211) - Adding several hosts via VMSSC creates a syslog entry only for the first host but no corresponding entries for rest of the hosts**

  This issue has been resolved and adding hosts via VMSSC creates syslog entries every time.

- **(SRV-16407) DSM RESTful API and VMSSC cannot delete a GuardPoint from a shared host**

  GuardPoints were configured on host shared between two domains. One of the GuardPoints was deleted from the shared host from one domain, and when an attempt was made to delete another GuardPoint on that same shared host from the other domain, the attempt failed.

This issue is now resolved, the DSM REST API and VMSSC utility have been fixed to ensure that they work as designed and deleting a GuardPoint from a shared host is successful when deleted from any of the domains that share the host.

- **(SRV-18214) - A restored DSM backup invalidated imported LDAP users**

  A DSM backup restored to the same DSM server without the **Include User(s)** option selected, invalidated administrators imported from LDAP, when in fact the existing users should continue to function as defined.

  This issue is now resolved and restoring a DSM backup without the **Include User(s)** option does not affect existing users.

- **(SRV-18091) - Source IP address for DSM login is not included in the logs**

  This issue is now resolved and the source IP address is available in the DSM logs as well as the supported Syslog formats.

- **(SRV-18246) DSM unable to contact shared host after upgrading the DSM software**

  After upgrading the DSM software, the DSM Security administrator created a new domain and added a shared host to the new domain. However, when the administrator attempted to create a GuardPoint on the shared host, the DSM returned the following error, “`Unable to contact host <`*`hostname`*`>. The agent is refusing connections`”

  This issue is now resolved and a GuardPoint can be created on a shared host added to a domain.

- **(SRV-18563) HTTP Error 500 returned when requesting node information by using the REST API call GET system/configs)**

  A combination of VMSSC and REST API calls were used to add and register hosts to the primary node. The REST API endpoint,

  ```
  GET /dsm/v1/system/configs
  ```

  was used to return role information about the node (primary or failover) but, intermittently returned HTTP error 500.

  This issue is now resolved and the DSM RESTful API has been enhanced to include the following endpoint to return the role of the node (primary or failover):

  ```
  GET /dsm/v1/system/configs/role
  ```

  It returns the following output:

  ```
  {
  “role” : “primary”
  }
  ```

- **(SRV-18633) Using VMSSC to add a syslog server to a domain failed**

  A DSM administrator tried to add a syslog sever to a domain using the VMSSC utility but, the newly added syslog server was not displayed on the domain’s syslog page on the GUI. Further inspection revealed that the syslog server had been added at the system level.

This issue is now resolved and the VMCSSC utility adds a specified syslog server to the requested level; system or domain.

- **(SRV-15298) - KMIP rekey operation only works the first time**

  The rekey operation for KMIP only works the first time it is attempted, subsequent attempts to rekey fail.

  This issue has been resolved and the rekey operation works whenever it is invoked.

- **(SRV-12365) - Cannot download the certificate chain from the KMIP server.**

  Earlier, with the DSM as a key manager with KMIP, you could not download the certificate chain from the KMIP server.

  This issue is now resolved and the certificate chain can be downloaded from the KMIP server.

- **(SRV-16623) - Certificate import from Nutanix hardware platform to a DSM KMIP domain failed due to an authentication failure**

  A DSM v5.3.1 system with a KMIP license and no domains, was upgraded to DSM v6.0 and a new domain created. The user tried to upload a Nutanix certificate but the upload failed with an authentication error.

  This issue is now resolved and a Nutanix certificate can be imported to a DSM KMIP domain.

- **(SRV-18074) - Unable to recreate a key with the same name after destroying it in a KMIP domain**

  After creating a key in a KMIP domain with a specific name, and then destroying that, a user cannot create a new key with the same name as the key that was just destroyed.

Known Issues

- **(SRV-9268) - DSM does not return key information in KMIP response payload**

  The KMIP specification supports a partial name structure for key names, however Vormetric DSM does not, and therefore when the key name value does not match the value in the KMIP table, the query fails.

  There is no workaround for this issue as partial key names are not supported.

- **(SRV-15082) - Failover nodes display as red on the primary HA page until synchronization is complete**

  HA replication status for failover DSM nodes is displayed as red while they are waiting to catch up with the primary DSM.

- **(SRV-15269) - DSM high availability with KMIP is now supported however, there is currently no UI support for this feature**

  You can configure high availability (HA) for a DSM with KMIP clients in the same way that you configure HA but, you need to restart the failover DSM node after replication between the primary and failover node is complete so that the KMIP clients can read relevant data from the failover node.

- **(SRV-15542) - Failover DSM node must be restarted when replication is complete**

  In a DSM HA configuration with KMIP, the failover DSM node must be restarted once replication is complete to ensure that the KMIP client can read the data from the failover node. To restart the server;

  a: Start a CLI session on the failover node, and restart the server as follows:

  b: At the CLI prompt, type the following;

  c:
  ```
  0001:vormetric$ system
  0002:system$ server restart
  ```

  d: Confirm the restart when prompted to do so.

- **(SRV-15374) - Bringing down a DSM IP link configured with an IPv6 address, removes that address**.

  When an IPv6 configured DSM Ethernet interface link is brought down using the CLI command
  ```
  ip link set {eth0|eth1} down
  ```
  the IPv6 address is lost. You will need to reconfigure the IPv6 address for that Ethernet interface when you bring it back up.

- **(SRV-14534 and SRV-15592) Cannot use a custom IPMI Web SSL port**

  The IPMI remote console cannot launch the Java application for the remote console if the web port is changed from the default 443 to a custom value.

  To fix this issue: In addition to changing the web port from the IPMI console Configuration settings, you must also edit the `.jnlp` file that launches the Java console.

  a: In the IPMI management console, click **Configuration > Port**

  b: Change the Web SSL port from 443 and click **Save**. You will lose connectivity to the IPMI console when you change the port number. Enter the URL to log in again with the new port number as; https://<*IP address or host name*>:<*Port number*>

  c: Navigate to **Remote Control > Console Redirection** and click **Launch Console**. Download the resulting `.jnlp` file. You need to edit the web port information in this `.jnlp` file. The first line in the file that contains the URL, needs to be edited to change the default port from 443 to the new port number.

  d: Save the file and then double-click the `.jnlp` file to launch the remote Java console.

Upgrade to Release 6, Version 6.0.1

DSM software version 6.0 is the minimum supported version that can be upgraded to DSM software version 6.0.1. Refer to the *DSM Installation and Configuration Guide* for details about how to upgrade your software.

We recommend that you backup your DSM configuration *before* you upgrade your DSM software.

DSM 6.0.1 Browser Support

The following browsers are supported:

- Internet Explorer 10, 11
- Firefox
- Chrome

DSM and Agent Compatibility

DSM and VTE Agent Compatibility

The following table shows compatibility between DSM version 6.0.1 and the VTE (FS) Agent versions:

Table 2: DSM and Agent software compatibility

DSM SW Version	Agent SW Version				
	5.2.3	**5.2.4**	**5.2.5**	**6.0**	**6.0.1**
5.2.3	Compatible	Compatible	Compatible	Compatible	Compatible
5.3.0	Compatible	Compatible	Compatible	Compatible	Compatible
5.3.1	Compatible	Compatible	Compatible	Compatible	Compatible
6.0	Compatible	Compatible	Compatible	Compatible	Compatible
6.0.1	Compatible	Compatible	Compatible	Compatible	Compatible

NOTE: If a 64-bit database is installed, you must install the 64-bit key agent. Installing the 32-bit key agent with 64-bit database is not supported.

DSM and VAE/VKM Compatibility

The following table shows compatibility between the DSM and VAE/VKM agent versions. Note that VKM is at v5.2.4.

Table 3: DSM and VAE/VKM Compatibility

DSM SW Version	Agent Version		
	5.2.3	5.2.4	5.2.5
5.2.3	Compatible	Compatible	Compatible
5.3.0	Compatible	Compatible	Compatible
5.3.1	Compatible	Compatible	Compatible
6.0	Compatible	Compatible	Compatible
6.0.1	Compatible	Compatible	Compatible

DSM and KMIP agent software version compatibility

The following table shows compatibility between the DSM software versions and KMIP protocol versions.

Table 4: DSM Software and KMIP support

DSM SW Version	KMIP Protocol Version Supported				
	1.0	1.1	1.2	1.3	1.4
5.2.3	Compatible	Compatible	Compatible	Not Compatible	Not Compatible
5.3.0	Compatible	Compatible	Compatible	Not Compatible	Not Compatible
5.3.1	Compatible	Compatible	Compatible	Not Compatible	Not Compatible
6.0	Compatible	Compatible	Compatible	Not Compatible	Not Compatible
6.0.1	Compatible	Compatible	Compatible	Compatible	Compatible

How to Get Help

For support and troubleshooting issues:

- http://help.thalesesecurity.com
- http://support.vormetric.com
- support@thalesesecurity.com
- (877) 267-3247

For Sales:

- http://go.thalesesecurity.com/contact-data-security-specialist-form.html
- sales@thalesesec.net
- (408) 433-6000

Notices and License

Vormetric Data Security Platform
Vormetric Transparent Encryption (VTE)

Protected by U.S. patents:
6,678,828
6,931,530
7,143,288
7,283,538
7,334,124
Vormetric Data Security includes a restricted license to the embedded IBM DB2 database. That license stipulates that the database may only be used in conjunction with the Vormetric Security Server. The license for the embedded DB2 database may not be transferred and does not authorize the use of IBM or 3rd party tools to access the database directly.