

# Veritas Access Software-Defined Storage (SDS) Management Platform Solutions Guide

Linux

7.4

# Veritas Access Software-Defined Storage (SDS) Management Platform Solutions Guide

Last updated: 2018-07-24

Document version: 7.4 Rev 0

## Legal Notice

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, Veritas InfoScale, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-Party Programs"). Some of the Third-Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the third-party legal notices document accompanying this Veritas product or available at:

<https://www.veritas.com/licensing/process>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC

500 E Middlefield Road  
Mountain View, CA 94043

<http://www.veritas.com>

## Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

<https://www.veritas.com/support>

You can manage your Veritas account information at the following URL:

<https://my.veritas.com>

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)

[CustomerCare@veritas.com](mailto:CustomerCare@veritas.com)

Japan

[CustomerCare\\_Japan@veritas.com](mailto:CustomerCare_Japan@veritas.com)

## Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The document version appears on page 2 of each guide. The latest documentation is available on the Veritas website:

<https://sort.veritas.com/documents>

## Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

[doc.feedback@veritas.com](mailto:doc.feedback@veritas.com)

You can also see documentation information or ask a question on the Veritas community site:

<http://www.veritas.com/community/>

## Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

[https://sort.veritas.com/data/support/SORT\\_Data\\_Sheet.pdf](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# Contents

Chapter 1	Introduction .....	6
	About Veritas Access .....	6
	About the SDS Management Platform .....	6
Chapter 2	Deploying the SDS Management Platform with Veritas Access .....	8
	Deploying the SDS Management Platform .....	8
Chapter 3	Using the SDS Management Platform interface .....	11
	Using the SDS Management Platform launchpad .....	11
	Using the Infrastructure application .....	13
	Using the Long Term Retention Storage (LTR) application .....	22
	Operation icons on the SDS Management Platform interface .....	24
Chapter 4	Setting up SSL in the SDS Management Platform .....	27
	About setting up SSL in the SDS Management Platform .....	27
	Generating and installing a new certificate .....	28
	Creating and upgrading a trust store .....	32
Chapter 5	Performing authentication .....	33
	Authentication modules .....	33
	Certificate-based client authentication .....	34
Chapter 6	System backup and restore .....	36
	About system backup and restore .....	36
	Automatic backups .....	37
	Manual backups .....	37

## Chapter 7

Troubleshooting .....	39
Log locations .....	39
Diagnostic reports .....	40
Java Virtual Machine (JVM) parameters .....	40
SDS Management Platform known issues .....	41
If multiple bucket creation requests with different inputs for attributes such as size and layout are in progress in parallel, then a bucket can get created with incorrect attributes .....	41
When editing a storage resource or backup server, an Advanced button is available that shows options that you should not change .....	41
If you add a Veritas Access cluster where the host includes the protocol (such as, https://10.20.30.40), the provider gets added and collects data but running the LTR workflow fails .....	41
When you create a bucket, the status of the task appears as DONE, even though the creation is still in progress .....	42
Clicking on a non-mapped Veritas Access cluster directs you to an empty wiki page which shows a table and some data .... 4   2	
If you restart the operating system, the SDS Management Platform does not start automatically .....	42
When you add a storage resource or backup server, the added resource is not automatically visible .....	42
After the SDS log is rotated, the log messages from either Veritas Access or the SDS plugin go to the rotated file instead of the new file .....	43
Some of the storage resources may appear as faulted and a warning sign appears next to the cluster IP address in the Infrastructure> Storage Resources page .....	43
Creation of STU fails if the S3 user is changed .....	43
Software limitations .....	43

# Introduction

This chapter includes the following topics:

- [About Veritas Access](#)
- [About the SDS Management Platform](#)

## About Veritas Access

Veritas Access is a software-defined, scale-out network-attached storage (NAS) solution for unstructured data that works on commodity hardware. Veritas Access provides resiliency, multi-protocol access, and data movement to and from the public and private cloud based on policies. You can reduce your storage costs by using low-cost disks and by storing infrequently accessed data in the cloud.

## About the SDS Management Platform

The Software-Defined Storage (SDS) Management Platform when integrated with Veritas Access provides a platform to integrate data from various sources within an enterprise (not just the data center), which presents a single, integrated view in to the whole environment. The SDS Management Platform brings together Veritas Access and Veritas NetBackup using a simple and intuitive platform to address long-term retention and other use cases.

The SDS Management Platform provides a platform for products like Veritas Access and Veritas NetBackup to work seamlessly to address your storage requirements. In the first iteration of the SDS Management Platform, you can manage Veritas Access and NetBackup deployments and address a critical use case for providing long-term retention storage for Veritas NetBackup using Veritas Access through a single interface. You can also provision and manage storage across your Veritas Access clusters using the power of SDS. In the future, other integrations for Veritas

products will be introduced using the SDS Management Platform with the goal of simplifying the user experience.

# Deploying the SDS Management Platform with Veritas Access

This chapter includes the following topics:

- [Deploying the SDS Management Platform](#)

## Deploying the SDS Management Platform

Supported operating system: RHEL 7.4

Supported NetBackup server versions: 8.1 and later

---

**Note:** If you are using NetBackup 8.1, you have to add a Veritas Access cloud instance. For more information, see [https://www.veritas.com/support/en\\_US/article.000125094](https://www.veritas.com/support/en_US/article.000125094).

---

### Prerequisite

- Ensure that you have installed Java version 1.8.0u152.  
You can find out the existing version of Java present in your system. If you have not installed Java, then, you can install it using the `yum install java-1.8.0-openjdk` command. If any other versions of Java are installed, you have to set the 1.8.0 version as the default.  
You can set the default using the `alternatives --config java` option and selecting the required version.
- Add Veritas Access cluster details to the `/etc/hosts` file of the NetBackup master server.



- The SDS Management Platform RPMs are available at  
 /dvd1-redhatlinux/rhel7\_x86\_64/fluidops/rpms.

You are required to install the following packages:

- RPM containing the core platform: `VRTSFOPS-platform-9.0.0.XXXX.noarch.rpm`
- RPM containing the modules for the SDS Management Platform (VDL branding, Infrastructure Application, Providers and the User Interface):  
`VRTSFOPS-bundled-sds-mgmt-platform-1.0.XXXX.rpm`
- RPM containing the Long Term Retention Storage application:  
`VRTSFOPS-bundled-sds-ltr-1.0.183.rpm`
- RPM containing the SDS module: `VRTSsds-fops-1.0.xxxxx.rpm`

### To deploy the SDS Management Platform

- 1 Install the core platform rpm.

```
rpm -Uv VRTSFOPS-platform*.rpm
```

- 2 Install the bundled application.

```
rpm -Uv VRTSFOPS-bundled-sds*.rpm
```

- 3 Install the SDS module.

```
rpm -Uv VRTSsds_fops*.rpm
```

- 4 Check whether all the SDS services are running using the following command:

```
/etc/init.d/sds_fops status
```

```
/etc/init.d/sds-access_fops status
```

- 5 Start the platform using the following command:

```
/etc/init.d/fops start
```

---

**Note:** The applications can be updated without updating the core platform.

---

- 6 Check whether all the services are running using the following command:

```
/etc/init.d/fops status
```

- 7 After you install the SDS Management Platform RPMs on any Veritas Access cluster node, you have to open the 50443 port. You can open the port using the following command:

```
iptables -I INPUT 1 -p tcp --dport 50443 -j ACCEPT
```

The SDS Management Platform server takes some time to start. Wait for a few minutes.

After installing the SDS Management Platform RPMs, you can verify if the 50443 port is open using the following command:

```
netstat -plunt | grep 50443
```

If the command does not return any output, then you have to reload the `systemctl` daemon and restart the SDS Management Platform server.

```
systemctl daemon-reload  
systemctl restart fops
```

- 8 After a few minutes, you can access the platform in a browser using the <https://<host>:50443> URL.
- 9 The default credentials are:

User: *admin*

Password: *5D5C+r1!*

You can change the password on the **User Management** page. Go to **Settings > User Management**.

# Using the SDS Management Platform interface

This chapter includes the following topics:

- [Using the SDS Management Platform launchpad](#)
- [Using the Infrastructure application](#)
- [Using the Long Term Retention Storage \(LTR\) application](#)
- [Operation icons on the SDS Management Platform interface](#)

## Using the SDS Management Platform launchpad

Once you log on successfully, the SDS Management Platform launchpad is the first interface that appears. The launchpad shows the applications that are installed. If you have installed only the base platform, no applications appear in the launchpad. When you select a specific application, you can see the content specific to your application.

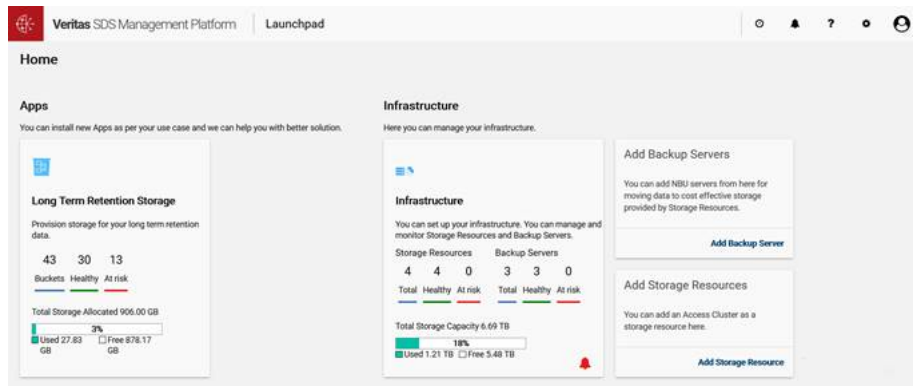
**Figure 3-1** SDS Management Platform workflow



In the current release, the two main applications that are available are the **Infrastructure** application and the **Long Term Retention Storage** application.

The menu is also specific to an application. The menu always includes **Back to Launchpad** as the first option. If you want to switch to a different application, you can go back to the launchpad using this menu option and select a different application in the launchpad.

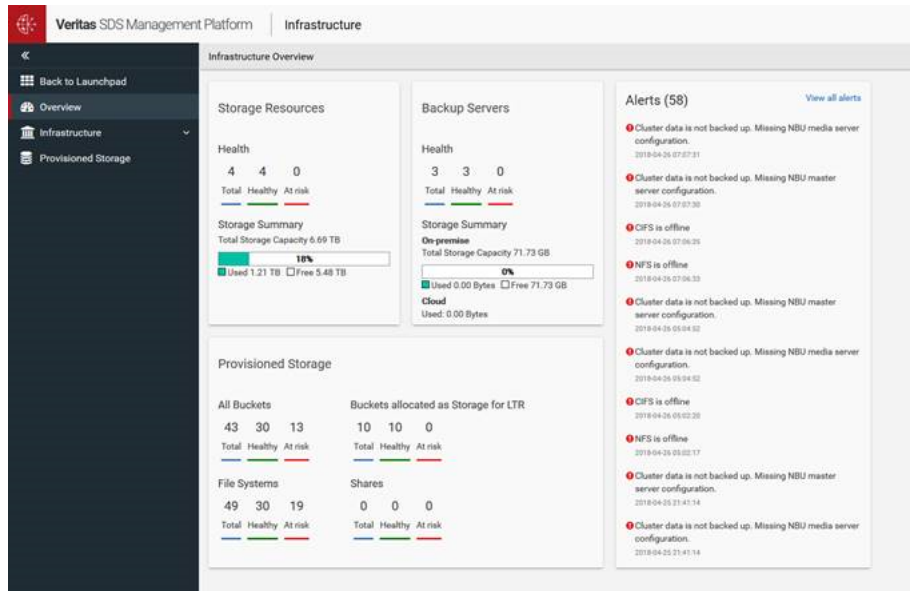
**Figure 3-2** SDS Management Platform launchpad



If you install the Veritas Access solution, you can see the **Add Backup Servers** and the **Add Storage Resources** pane.

## Using the Infrastructure application

This section describes the **Infrastructure** application.

**Figure 3-3** Infrastructure application

The Infrastructure application has the following menu entries:

- [Back to Launchpad](#)
- [Overview](#)
- [Infrastructure](#)
- [Provisioned Storage](#)

## Back to Launchpad

Use this option to go back to the launchpad and switch to another application.

## Overview

This page displays the following information:

- Displays the health and storage overview for the storage resources and the backup servers.  
The storage summary shows the storage utilization of all the Veritas Access clusters and the NetBackup servers.  
You can interpret the storage summary as follows:

- |         |   |
|---------|---|
| Total   | The total number of Veritas Access clusters (storage resources) and NetBackup servers (backup servers) known to the platform. |
| Healthy | If data is collected successfully from the system, the system is healthy.   |
| At risk | If no connection is established with the system, the system is at risk.   |
- Health overview for provisioned storage.  
Displays the details for all the buckets, the buckets that are used as LTR storage, file systems, and shares. A resource is denoted as healthy if the resource is online or in running state. Otherwise, the resource is said to be at risk.
  - Alert overview  
Lists the alerts coming from the Veritas Access installation. Only a limited number of alerts are shown on the **Overview** page. The alerts are sorted by severity and date. You can view all the alerts by selecting **View all alerts**.

Infrastructure

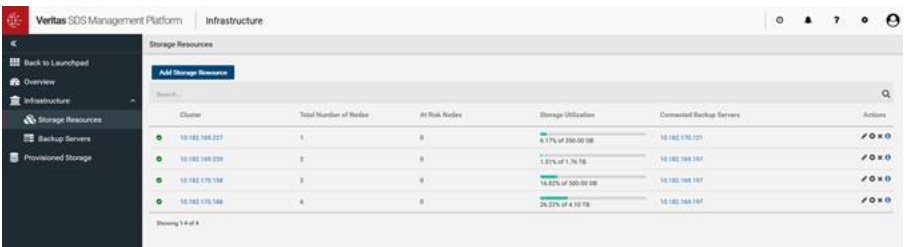
This has two sub-menu items:

- Storage Resources
- Backup servers

Storage Resources

This page shows an overview of the Veritas Access clusters known to the platform.

Figure 3-4 Storage Resources



You can see the following information:

- An icon shows whether the cluster is at risk or healthy. For each cluster, details such as the total number of nodes, number of nodes at risk, storage utilization, and the connected backup servers are shown.

- You can perform the following actions on a cluster:
  - Edit the provider that collects data from the Veritas Access installation.  
For example, you can change the password that is required to log on to Veritas Access.
  - Delete all the data for the Veritas Access cluster and the provider that collects the data.
  - Run the provider.
- The information icon shows when the data was last collected, the duration of the data collection, and if there were any errors during the last provider run and how much data was collected.
- You can add a new Veritas Access cluster using the **Add Storage Resource** option.



## To add a new storage resource

- 1 Click on **Add Storage Resource**.
- 2 In the pop-up window, enter the host name or IP address of the Veritas Access cluster (or the management console), the credentials (master user name and password needed to log on to Veritas Access), and the port number of the Veritas Access installation (the default port number is already pre-set, but can be changed if needed).

If you have enabled S3 on the Veritas Access cluster and the S3 bucket user is different from the user name provided in the credentials, you have to provide the S3 bucket user credentials. Else, you can ignore these fields.

If you want to immediately validate your configuration details (before the provider is added) , check the **Validate provider** checkbox.

Add Storage Resource

Host \*

Port \*

14161

User \*

Password \*

Fields with a \* are required.

If S3 is enabled on the Access cluster and the S3 bucket user is different from the user provided above, the credentials of the S3 bucket user need to be provided below. Otherwise the fields can be left empty.

S3 Bucket User

S3 Bucket Password

Validate provider

☒ ⓘ

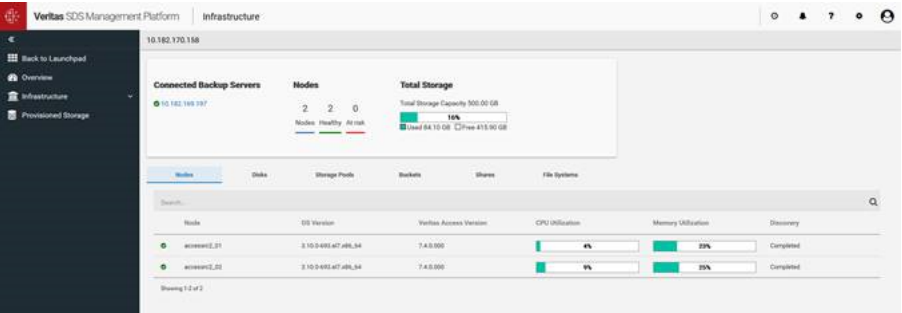
Submit

- 3
- After you submit the form, a provider is created that tries to collect data from the Veritas Access installation. If this is successful, the Veritas Access cluster is listed in the table that lists the storage resources. Go to **Infrastructure > Storage Resources** to verify if the new storage resource appears in the table.

**Note:** You have to reload the page after a short waiting period to see this information. If a connection to the Veritas Access cluster cannot be established, a notification is shown above the table. You have the option to edit the provider to fix the issue. For example, you can re-enter the password or to delete the provider.

You can get more details on a specific Veritas Access cluster by clicking on it. The detail page of a specific Veritas Access cluster shows an overview of the cluster at the top. There are tables for the nodes, disks, storage pools, buckets, shares, and file systems of the cluster showing detailed information. Even if one of these resources is at risk, a red exclamation mark appears in the tab of the respective resource.

Figure 3-5 Storage Resources details



Backup servers

This page shows an overview of the NetBackup servers known to the platform.

Figure 3-6 Backup Servers



You can see the following information:

- A table shows the details for each NetBackup server, such as the health status of the server (whether the platform can collect data from the server), the total number of NetBackup policies and the number of policies in use, the connected storage resources, and the storage utilization.
- You can perform the following actions on a server:
  - Edit the server that collects data from the NetBackup server.  
For example, you can change the password that is required to log on to Veritas Access.
  - Delete all the data for the Veritas Access cluster and the provider that collects the data.
  - Run the provider.
- You can add a new NetBackup server using the **Add Backup Server** option.

### To add a new backup server

- 1 Click on **Add Backup Server**.
- 2 In the pop-up window, enter the host name or IP address of the NetBackup server, the credentials (user name is **root** and password needed to log on to NetBackup server), and the port number (the default port number is already pre-set, but can be changed if needed).

Add Backup Server

Host \*

Port \*

User \*

Password \*

Validate provider ☒ ⓘ

fields with a \* are required

Submit

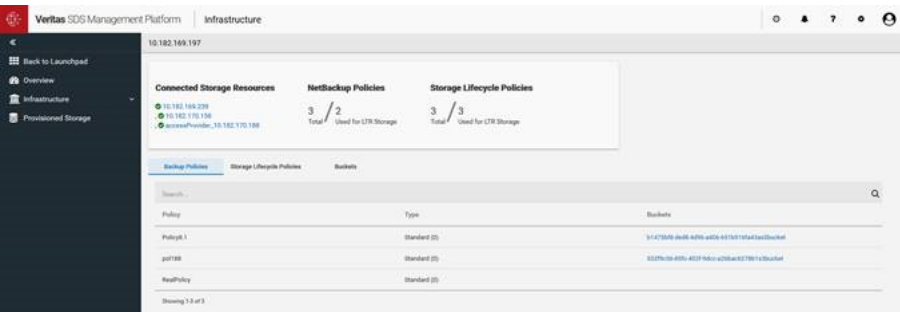
- 3 After you submit the form, a provider is created that tries to collect data from the NetBackup server. If this is successful, the backup server is listed in the table that lists the backup servers. Go to **Infrastructure > Backup Servers** to verify if the new backup server appears in the table.

---

**Note:** You have to reload the page after a short waiting period to see this information. If a connection to the Veritas Access cluster cannot be established, a notification is shown above the table. You have the option to edit the provider to fix the issue. For example, you can re-enter the password or to delete the provider.

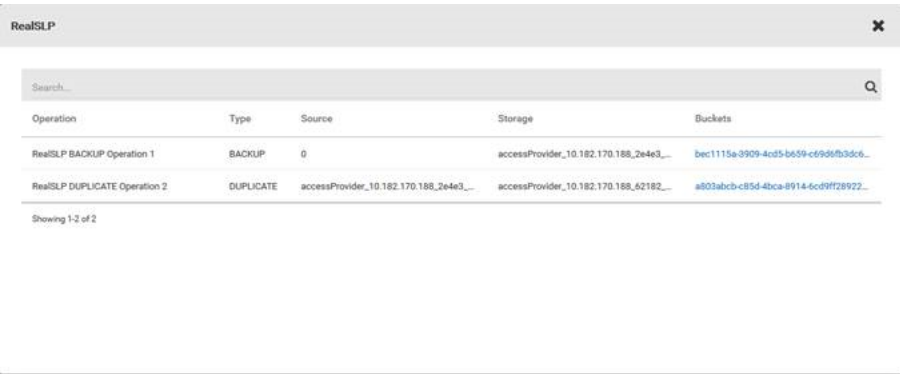
---

Figure 3-7 Backup Server details



You can get more details on a specific NetBackup servers by clicking on it. The detail page of a NetBackup server shows an overview at the top and shows the connected storage resources, total number of NetBackup policies, and how many are used for LTR.

Figure 3-8 SLP details



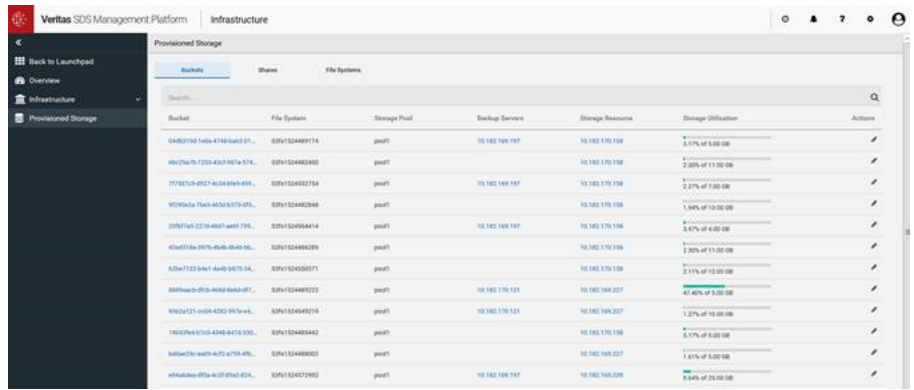
The table has three tabs that gives the following details:

- Backup Policies: Lists the policy name, policy type, bucket (if the bucket has been used with the respective policy in LTR) .
- Storage Lifecycle Policies: Lists the policy name and policy type. When selecting the information icon, a popup shows the information on the operations of the policy, the operation type, source, and storage unit (STU).
- Buckets and their storage utilization.

## Provisioned Storage

This page lists all the buckets, shares, and the file systems of all the known Veritas Access clusters.

**Figure 3-9** Provisioned Storage

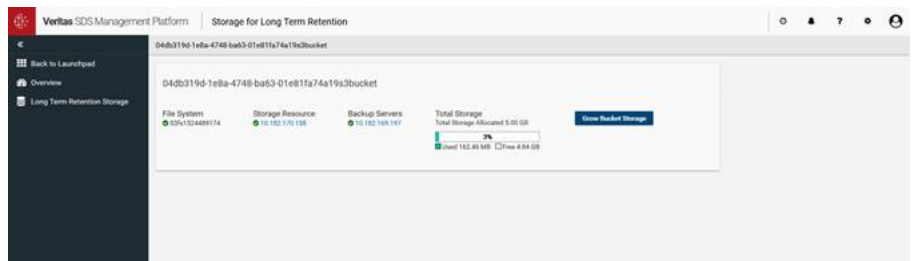


Bucket	File System	Storage Pool	Backup Servers	Storage Resource	Storage Utilization	Actions
04db319d-1eba-4748-ba63-01e811a74e19s3bucket	SDX1024489174	pool1	10.182.169.197	10.182.170.138	3.17% of 5.00 GB	
48a27a76-1203-43a1-987a-537a	SDX1024489174	pool1	10.182.170.138	10.182.170.138	2.08% of 11.00 GB	
773870c1-4927-a63a-8b6a-489c	SDX1024489174	pool1	10.182.169.197	10.182.170.138	2.27% of 7.00 GB	
9029a5a1-7a65-a65a-6275-487a	SDX1024489174	pool1	10.182.170.138	10.182.170.138	1.94% of 10.00 GB	
2207a7a5-2274-4a67-aad7-719c	SDX1024489174	pool1	10.182.169.197	10.182.170.138	5.41% of 4.00 GB	
43a010a1-997a-4b4b-4b4b-4b4b	SDX1024489174	pool1	10.182.170.138	10.182.170.138	2.30% of 11.00 GB	
43a010a1-997a-4b4b-4b4b-4b4b	SDX1024489174	pool1	10.182.170.138	10.182.170.138	2.11% of 10.00 GB	
889ba0b1-0f0a-4b4b-4b4b-4b4b	SDX1024489174	pool1	10.182.170.138	10.182.169.227	47.40% of 5.00 GB	
19a2a121-c004-430d-997a-e4c1	SDX1024489174	pool1	10.182.169.227	10.182.170.138	1.07% of 10.00 GB	
19a2a121-c004-430d-997a-e4c1	SDX1024489174	pool1	10.182.170.138	10.182.170.138	3.17% of 5.00 GB	
5a05a020-aad7-a759-4b5c-4b5c	SDX1024489174	pool1	10.182.169.227	10.182.170.138	1.81% of 5.00 GB	
9f4a4a0a-0f0a-4b4b-4b4b-4b4b	SDX1024489174	pool1	10.182.169.227	10.182.169.227	0.84% of 25.00 GB	

You can get more details on a specific bucket by clicking on it

The bucket page shows an overview of the bucket and provides an option to grow the bucket storage.

**Figure 3-10** Bucket details



File System	Storage Resource	Backup Servers	Total Storage
SDX1024489174	10.182.170.138	10.182.169.197	5.00 GB

Used 163.48 MB 3% Free 4.84 GB

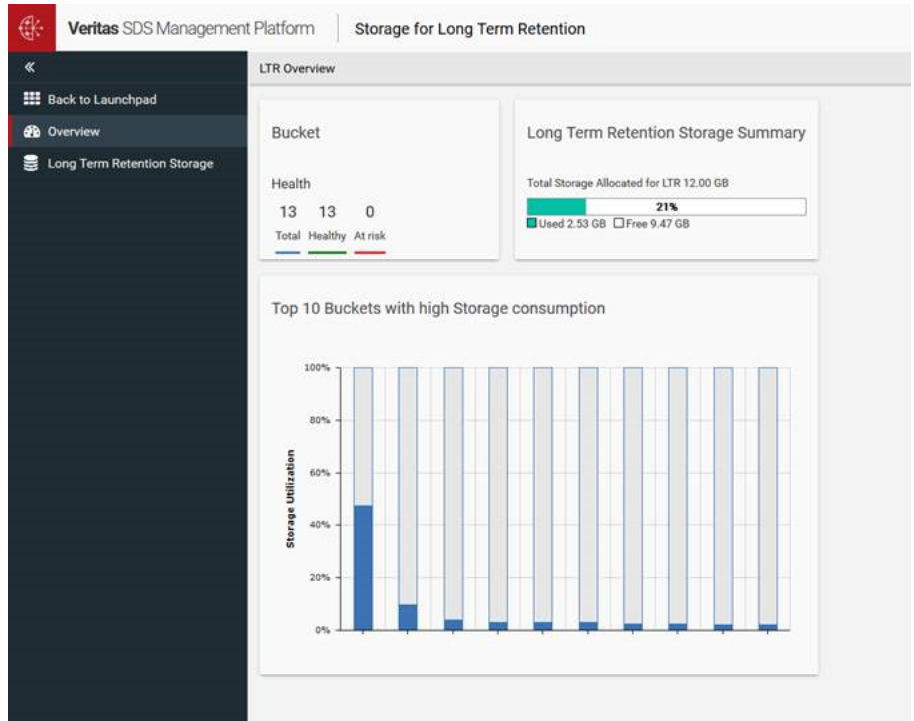
## Using the Long Term Retention Storage (LTR) application

The LTR application has the following menu entries:

- **Back to Launchpad**  
Use this option to go back to the launchpad, and switch to another application.
- **Overview**  
Displays the bucket health overview, storage utilization, and a bar chart showing the top ten buckets with the highest storage utilization. An alert overview with LTR-specific alerts is also displayed, if the details are available.
- **Long Term Retention Storage**

Shows a table of all the buckets with information on the file system, storage pool, backup server (if the bucket is used for LTR), storage resource, and storage utilization.

**Figure 3-11 Long Term Retention Storage application**



You can use the **LTR** wizard to configure storage for long-term retention.

#### **To configure storage for long-term retention using the LTR wizard**

- 1 Click on **Provision Storage** to start the LTR wizard. An infographic for the LTR workflow appears on the screen.
- 2 All the NetBackup servers known to the platform are shown in a table. Select any one server.
- 3 All the backup policies of the selected NetBackup server are shown in a table. Select any one policy.
- 4 Select whether you want to use an existing bucket for LTR or create a new one by choosing either **Select existing bucket** or **Create new bucket**.

If you select **Select existing bucket**, all the available buckets are listed in a table. Select any one bucket.

If you select **Create new bucket**, you are prompted to enter the following details:

- Bucket size: The size of the bucket to be created.
- File system layout: Select any one of the values - **mirrored**, **simple**, or **erasure-coded** from the drop-down menu.
- Device protection: If you have selected **erasure-coded** as the file system layout, select either **disk** or **node** from the drop-down menu. If any other file system layout has been selected, you can ignore this field.
- Policy: **LTR On-premises** is pre-selected. Currently, you cannot change this value.

**5** A summary report is displayed that shows all the details.

The SDS module creates the bucket intelligently on the available clusters based on your inputs.

The bucket size can be increased either directly on the **Long Term Retention Storage** page using the respective action in the table or on the detail page of a bucket.

---

**Note:** The SDS module updates the `/etc/hosts` system file with the IP of the Veritas Access cluster.





---

## Operation icons on the SDS Management Platform interface


[Table 3-1](#) describes the operation icons visible on the SDS Management Platform interface.



**Table 3-1** Operation icons on the SDS Management Platform interface

Icon	Name	Description
	Job	<p>Displays a log of various actions on the system. The details include the description of the job, run time, start time, progress status, and messages (informational about actions that are performed or errors that have occurred), and the user who has performed an action.</p> <p>The progress status can be:</p> <ul style="list-style-type: none"> <li>■ The percentage of the progress if the job is still running.</li> <li>■ Done, if the job is successful.</li> <li>■ Error, if there was an error during execution.</li> </ul>
	Event	Displays the events collected from the Veritas Access installations.
	Help	Displays the available documentation.
	Settings	<p>Links to the following pages:</p> <ul style="list-style-type: none"> <li>■ <b>User Management:</b> You can add and delete users and change passwords. Veritas recommends that you change the default admin password after you log in for the first time.</li> <li>■ <b>Backup:</b> You can create or restore backups for the database of the platform.</li> <li>■ <b>Authentication set up:</b> You can configure authentication options for the platform. For example, you can configure whether authentication against LDAP should be used.</li> <li>■ <b>SSL configuration:</b> You can configure the SSL configuration for the web server and API.</li> <li>■ <b>Diagnostic Information:</b> You can collect the information required to diagnose problems and get product support.</li> </ul>

**Table 3-1**                      Operation icons on the SDS Management Platform interface  
*(continued)*

Icon	Name	Description
	Account	Links to the account page and the logout option.

User Management

You can also add ACLs for different users.

- If the user belongs to the **SDS LTR User** group, then the user has access only to the LTR application.
- If the user belongs to the **Access Infrastructure User** group, then the user has access only to the Infrastructure application.
- If the user is an **admin**, then the user has access to all applications and can perform any operation.

**Figure 3-12**                      User Management page



# Setting up SSL in the SDS Management Platform

This chapter includes the following topics:

- [About setting up SSL in the SDS Management Platform](#)
- [Generating and installing a new certificate](#)
- [Creating and upgrading a trust store](#)

## About setting up SSL in the SDS Management Platform

SDS Management Platform instances can be set up to authenticate and communicate securely amongst themselves using SSL certificates. The SSLs can be publically signed or self-signed certificates from your own CA (Certificate Authority). In the case of publically signed certificates, Internet access may be required to verify the authenticity of the certificate. The SDS Management Platform can make use of any certificates compatible with X509 and Java, but Veritas recommends the use of Privacy Enhanced Mail (PEM) certificates. The certificates are stored in a local Java keystore in each installation instance. In the SDS Management Platform, we distinguish between certificates of the HTTP(S) web server and internal API communication. For both configurations, distinct sets of keystores are used.

# Generating and installing a new certificate

You can generate certificates in many different ways. Veritas recommends using the KeyStore Explorer, a graphical UI for the Java Keytool. You can also use the Java Keytool.

## Using KeyStore Explorer to generate a new certificate

You can generate and install a new certificate in the SDS Management Platform using the KeyStore Explorer.

### To generate and install a new certificate with the KeyStore Explorer

- 1 Open the **KeyStore Explorer**.
- 2 You are prompted to select the type of the new KeyStore. Select **JKS**. Click **OK**.
- 3 Generate a new key pair. Right-click > **Generate Key Pair**.  
It is recommended to use RSA with a size of 2048 bits.
- 4 Configure the certificate settings.
  - It is recommended to use SHA256 with RSA (or stronger) as the signature algorithm. Modern browsers do not support MD5 or SHA-1 RC4.
  - Choose a suitable validity period.
  - A serial number is generated automatically.
  - Give a suitable name. Click on the address book icon to add name entities.
- 5 Add Subject Alternative Names (SANs).  
As mentioned in RFC 2818, the use of CN to match the host's identity is deprecated and SAN should be used instead. To do this, click on **Add Extensions** in the certificate settings dialog, add an extension with the plus icon and choose **Subject Alternative Name** as the extension type. In the dialog, add at least one DNS entry that matches the host name to access the SDS Management Platform.
- 6 Enter the alias.  
Veritas recommends using **jetty** as the alias though this is not strictly required. You can externally configure the actual alias that is used by the web server.
- 7 Enter the key pair password.

---

**Note:** The password of the keystore and the key need to be the same

---

- 8 Check the certificate details. Double-click on the key pair in the list to see its properties. Also check that the Subject Alternative Names are visible in the extensions.
- 9 Generate CSR. Right-click on the certificate -> **Generate CSR**.
- 10 Send the CSR to a certificate authority and let it be signed.
- 11 Import the CSR response. Right-click on the certificate-> **Import CA Reply > From File**.

---

**Note:** If your CA is not globally trusted (for example, if you see an error message such as, **Could not establish trust** while importing the CA reply), you need to import the CA certificate as a trusted certificate. Right-click > **Import trusted certificate**.

---

- 12 Save the keystore (for example, *mykeystore*) and use the same password that you used for the key.

Once the keystore is created, it can be activated as follows:

- Place the keystore into the `etc` folder of the installation (example, `etc/mykeystore`).
- Adjust the `config.prop` settings.

```
httpKeyStore=etc/mykeystore
httpKeyStorePassword=fluidops
```

The key for the RMI communication can be generated and installed accordingly. The key (or the CA) has to be part of the corresponding trust store to establish the SSL trust.

## Using the Java Keytool to generate a new certificate

The Java Keytool is a command-line tool for certificate management that is bundled with the JDK. The SDS Management Platform bundles a JRE in the installation folder.

- Generate keys.

This creates a new key pair in a new or existing Java Keystore, which can be used to create a CSR, and obtain an SSL certificate from a Certificate Authority (CA). The following command generates a 2048-bit RSA key pair, under the specified alias (domain), in the specified keystore file (`keystore.jks`):

```
keytool -genkeypair -alias <domain> -keyalg RSA -keystore keystore
```

If the specified keystore does not already exist, it is created after the requested information is supplied. You are prompted for the keystore password (new or existing), followed by a Distinguished Name prompt (for the private key), then the desired private key password.

If you want your certificate to not only accept the given common name but rather additional names or IPs, you can use the keytool's SAN (Subject Alternative Names) extension.

```
keytool -genkeypair -alias <domain> -keyalg RSA -keystore keystore  
-ext SAN=dns:example.com,dns:localhost,ip:127.0.0.1
```

- Generate CSR for existing private key.

Use this method if you want to generate a CSR that you can send to a CA to request the issue of a CA-signed SSL certificate. It requires that the keystore and alias already exist. You can use the previous command to ensure this. You can use the following command to create a CSR (`domain.csr`) signed by the private key identified by the alias (`domain`) in the (`keystore.jks`) keystore:

```
keytool -certreq -alias <domain> -file <domain.csr> -keystore keystore
```

After you enter the keystore's password, the CSR is generated.

- Import signed or root certificate.

Use this method if you want to import a signed certificate, for example, a certificate signed by a CA, into your keystore; it should match the private key that exists in the specified alias. You may also use this same command to import root or intermediate certificates that your CA may require to complete a chain of trust. Specify a unique alias, such as `root` instead of `domain`, and the certificate that you want to import. You can use the following command to import the certificate (`domain.crt`) into the keystore (`keystore`), under the specified alias (`domain`). If you import a signed certificate, it should correspond to the private key in the specified alias.

```
keytool -importcert -trustcacerts -file <domain.crt> -alias <domain>  
-keystore keystore
```

You are prompted for the keystore password, and for a confirmation of the import action.

Make sure that the original certificate used to create the CSR is removed from the keystore, otherwise it will be confused with the imported signed certificate. You may also use the command to import a CA's certificates into your Java truststore, which is typically located in `$JAVA_HOME/jre/lib/security/cacerts` assuming `$JAVA_HOME` is where your JRE or JDK is installed. If you want to import root and intermediate certificates, they have to be imported in one go. If

they are located in several files, their content has to be merged into a single file before they can then be imported.

- Generate a self-signed certificate in a new or existing keystore.  
Use this command if you want to generate a self-signed certificate for your Java applications. This is the same command that is used to create a new key pair, but with the validity lifetime specified in days. The following command generates a 2048-bit RSA key pair, which is valid for 365 days, under the specified alias (domain), in the specified keystore file (*keystore*):

```
keytool -genkey -alias <domain> -keyalg RSA -validity 365 -keystore  
keystore
```

If the specified keystore does not already exist, it is created after the requested information is supplied. You are prompted for the keystore password (new or existing), followed by a Distinguished Name prompt (for the private key), then the desired private key password.

- Convert a certificate in `pfx` format to `pem` and import it to the keystore.  
You can convert a certificate and import it to the keystore using the keytool.

```
keytool -importkeystore -srckeystore ECMTEST_BAP.pfx -srcstoretype  
pkcs12 -destkeystore clientcert.jks -deststoretype JKS
```

- List the contents of a keystore.  
To list the keystore contents, use the following command:

```
keytool -list keystore keystore
```

```
Enter keystore password:
```

```
Keystore type: JKS
```

```
Keystore provider: SUN
```

```
Your keystore contains 1 entry
```

```
jetty, Feb 4, 2009, PrivateKeyEntry,
```

```
Certificate fingerprint (SHA1): 5B:4D:....
```

- You can import another certificate using **either** of the following commands:
  - `keytool -keystore keystore -import -alias jetty -file YOURCERTIFICATE -trustcacerts`

```
■  
keytool -importkeystore -srckeystore YOURKEYSTORE -srcstoretype PKCS12  
-destkeystore keystore
```

## Creating and upgrading a trust store

A trust store defines the certificates of authorities that are generally trusted. The SDS Management Platform ships a default API trust store that contains the root certificates of the JDK, as well as the self-signed certificate used in default installations. Veritas recommends that you create such a trust store based on an existing trust store.

When you perform an upgrade, custom trust stores are copied over to the new installation. Unmodified bundled trust stores are automatically upgraded. If during an upgrade, the installer detects that the bundled trust store was modified, it is copied over to the new installation, and the new version is kept with a `.original` extension.



# Performing authentication

This chapter includes the following topics:

- [Authentication modules](#)
- [Certificate-based client authentication](#)

## Authentication modules

The SDS Management Platform implements a powerful security concept that supports different directory services. The authentication mechanism is associated with a role concept. There are different authentication modules and this section gives best practices for their configuration.

An authentication module authenticates users against a specific directory service. The SDS Management Platform supports the following authentication modules:

- [Local SDS Management Platform users](#)
- [LDAP Authentication](#)

These modules can be combined into an authentication chain. The SDS Management Platform evaluates the modules in the configured order until one module succeeds or all of them have failed. If one of the modules is not configured properly, it is ignored and the evaluation continues with the next module in the chain.

### Local SDS Management Platform users

This authentication module lets you authenticate the local SDS Management Platform users. Within the **authConfigOptions** parameter, you can specify an optional value called the *local.domain* value. When this value is set, the user needs to specify this value as the domain during authentication. The passwords of local users are hashed by default. The configuration setting, *hashUserPasswords* can be used to change the default behavior.

## LDAP Authentication

This module lets you authenticate users against an LDAP server. The location of the server is configured with the *authConfigOptions* parameter. You can either use the **Authentication** Wizard or compile the configuration string manually.

<code>ldap.url</code>	Specifies the LDAP server's URL, for example <a href="#">ldap://my.ldap.server:389</a> . You cannot specify the LDAP endpoint using the IP address. You can specify the LDAP endpoint only by a fully qualified domain name. If you want to authenticate against an Active Directory where the users are in the global catalog, use port 3268.
<code>ldap.domain</code> (OPTIONAL)	Specifies the LDAP domain. If specified, only users with the exact domain are allowed.
<code>ldap.admingroup</code> (OPTIONAL)	Specifies the admin group (defaults to Administrators) within the domain. Can be used to specify other admin groups (for example, if localized names are in place).

Example configuration string:

```
authConfigOptions=ldap.url\=ldap\://mt.company.corp\:389, ldap.domain\
=my.company.corp, ldap.guestgroup\=LDAPGuests,
ldap.admingroup\=LDAPAdmins:LDAPManagement,
ldap.sesusergroup\=LDAPEXternalUsers
```

It is possible to customize the rights of user groups using the LDAP module. To use authentication, each LDAP group that is granted access must be mapped to an SDS Management Platform group. This mapping is a prerequisite for you to be able to log on to the system.

## Certificate-based client authentication

The SDS Management Platform supports HTTP SSL certificate-based client authentication. If enabled, it is activated on an additional port in the web server (default: 50444), and clients must provide a valid certificate that is accepted by the web server.

You can configure a certificate-based client using the following settings:

Table 5-1

Settings	Description
<code>enableHttpSslCert</code>	Enables HTTP SSL certificate-based authentication for the web server. If enabled, certificate-based authentication is activated on the configured <code>httpSslCertPort</code> .
<code>httpSslCertPort</code>	Secures (SSL) HTTP port for certificate-based authentication to the web interface. Default: 50444
<code>httpTrustStore</code>	SSL TrustStore used by the web server. For example, for client-based certificate authentication, see <code>enableHttpSslCert</code> setting. Default: <code>etc/truststore</code>
<code>httpTrustStorePassword</code>	SSL TrustStore password used by the web server.
<code>httpKeyStore</code>	SSL KeyStore used by the web server. Default: <code>etc/keystore</code>
<code>httpKeyStorePassword</code>	SSL KeyStore password used by the web server.

By default, the SDS Management Platform ships an empty TrustStore. To establish trust, a valid CA certificate must be added to the TrustStore; alternatively, an existing trust store can be used.

---

**Note:** Certificate-based authentication can only be activated if the configured TrustStore contains at least one valid certificate. According to the protocol, clients require a certificate that is signed by a trusted CA.

---

To import a public CA key to an existing TrustStore, you can use the following command:

```
keytool -import -v -trustcacerts -alias my_ca -file ca.crt -keystore truststore
```

# System backup and restore

This chapter includes the following topics:

- [About system backup and restore](#)
- [Automatic backups](#)
- [Manual backups](#)

## About system backup and restore

The system state consists of:

- User Resource Description Framework (RDF) data
- Imported data
- Configuration
- Wiki edits
- Credentials (stored in the encrypted file `secrets.xml`)

You can obtain the imported data from the respective source, but provider parameters, user passwords, and other information required for the individual instance are recorded in various files that are present in the installation folder. All of these customer-specific configuration files should be backed up once the installation and configuration is completed, or whenever any updates are made. By default, this is done automatically by the system service itself every hour.

# Automatic backups

Complete data backups are performed automatically at regular intervals by the system. The backup path, interval, and number of backups to keep are specified with the following configuration parameters:

- `backupPath`
- `backupFrequencyInHours`
- `numberOfBackupsToKeep`

By default, these parameters are written to a local disk folder called `backup`, which is located parallel to the installation folder, once every hour, with a rolling window of 100 backups. The oldest backups are removed automatically once the number is arrived at. You can specify the backup path to use a mounted network share rather than the local disk. The service owner or user should have write privileges on that target. Very large data centers can produce large backup files that may consume all the available space on the disk. Hence, the backup folder or disk should be dimensioned accordingly, or the number of retained backups reduced accordingly.

---

**Note:** The backups are of the data only, not the software installation.

---

The automatic backup is a folder named with a date and timestamp, containing zip files, and all the configuration files required to restore the object database, the RDF datastore, and all instance-specific configuration parameters, providers, and authentication data. The object database (which is in-memory at run-time) is saved to the `db-core.zip` file, and the RDF datastore, wiki pages, and ontology are saved in the `timestamp_diagnosticfeedback.zip` file. These files collectively offer a consistent backup set from which the data can be restored to the time of the backup.

---

**Note:** The in-memory DB is persisted at intervals of one minute in between the hourly backups to `/db/dbcore.zip.temp.#`. If these files are still available after an incident, there is no loss of persisted data. However, all of the data that has originated from providers is reloaded at the next provider run if it is no longer in the database. Hence, it is not critical to maintain the data in this database from backups.

---

## Manual backups

You can take a manual backup of the system at any time using the `backup` command from the CLI. The backup is available in the standard format at `/backup/timestamp/dbcore.zip`.

You can backup the semantic datastore using the following command:

```
getSemanticService getbackupService backupDBs
```

The backup is available in the standard format in the `/backup/ date-timestamp/ date-timestamp_diagnosticfeedback.zip` folder. This functionality is also available through **Settings -> Backup**. The backup mechanism allows for saving the database at any time and restoring it when needed. You can save the history repository or the central database by selecting the type of backup. You have an option to make a diagnostic feedback backup. The diagnostic backup saves the database, the history repository, wiki pages, the `config` folder, and the `config.prop` file. This can be kept for later use or downloaded for making a diagnosis about the application.

You can also take a full backup which save all the data, pages, and configuration of the SDS Management Platform.

### To take a manual backup

- 1 Go to **Settings -> Backup**.
- 2 Select the database that you want to back up from the menu. Select **dbmodel** if you want to backup the main database where imported and authored triples are stored. Select **historymodel** if you want to backup the database that stores the historical data that is created by the historical data provider.
- 3 Click **Backup**. The backup of the database is available and can be used in the future to restore the database to the current state or be downloaded as a `.trig` file.

# Troubleshooting

This chapter includes the following topics:

- [Log locations](#)
- [Diagnostic reports](#)
- [Java Virtual Machine \(JVM\) parameters](#)
- [SDS Management Platform known issues](#)
- [Software limitations](#)

## Log locations

Messages related to the platform are logged to specific log files in the `Install Folder/logs` file. You can decide the number of log files to keep before recycling them by changing the `MaxBackupIndex` parameter in the `Install Folder/etc/log4j.properties` file.

- The `wrapper.log` contains information pertaining to the service start.
- The `startup.log` shows the product version and start parameters for the Java Virtual Machine (JVM) in which the system runs.
- The `service.log` shows all current messages relating to the started and running service, and is the main source of information for troubleshooting.
- The `service.log.#` are older incarnations that are cycled through 20 files before they are deleted automatically.
- The `job.log` lists all the transactions performed by the system and can be used for auditing purposes.
- The `datestamp-request.log` shows UI page requests.
- The `performance.log.#` details performance statistics relating to the service.

- The `rule-engine.log.#` shows rule engine runs and the time required for them to complete.
- The `install.log` records information from updating the system or when installing a solution.
- The `/var/log/sds_fops.log` shows the logs related to the SDS module.

## Diagnostic reports

You can trigger the diagnostic report from **Settings ->Diagnostic Information**. It is a general-purpose tool that streamlines the interaction with the SDS Management Platform support. The backend service runs within a Java Virtual Machine (JVM), that in turn runs within a service wrapper which ensures that the JVM is kept running. The service is normally started and stopped using the Windows `services.msc` or by a Linux `service init` script. If the service has completely stopped responding, first attempt to connect to the service using the Command Line Interface (CLI) and, if this is possible, produce a diagnostic feedback zip file (which causes the in-memory DB to be persisted) with the following command:

```
# getDiagnosticService createDiagnosticFeedback -addMemoryDump false
```

The diagnostic zip file is written to the `/webapps/ROOT/diag` folder and is named `diag+ timestamp.zip`. This causes the in-memory DB and the RDF triple store to be written to disk. Then, try to restart the service within the CLI using the `restartService` command. If all else fails, shutdown the operating system cleanly and restart. The database is always written in a consistent way, so it should always be readable.

## Java Virtual Machine (JVM) parameters

The main Java VM parameters are defined in the `backend.conf` file. You can find the JVM parameters in the `%INSTALL_DIR%/backend.conf` folder. The most frequent use case is to assign more memory to the backend process.

- `wrapper.java.additional.10=-Xmx3G`
- `wrapper.java.additional.4=-XX:MaxPermSize=256m`

Veritas recommends that you apply the user changes in the `backend-user.conf` file by defining new values for the respective settings.



# SDS Management Platform known issues

This section describes known issues related to the SDS Management Platform.

If multiple bucket creation requests with different inputs for attributes such as size and layout are in progress in parallel, then a bucket can get created with incorrect attributes

If you try to create multiple buckets in parallel, wherein you have different inputs for attributes such as size and layout, then it is possible that a bucket is created with attributes that are specified for some other bucket. This happens because there is a race condition between setting bucket attributes and creating bucket operations.

**Workaround:**

If you want to create multiple buckets in parallel, ensure that you verify that the bucket has been created with the correct attributes. If there is a mismatch, recreate the bucket.

When editing a storage resource or backup server, an **Advanced** button is available that shows options that you should not change

When editing a storage resource or backup server, an **Advanced** button is available which shows options that you are not required to change. The dialogs are generic for different kinds of integrations where these options are sometimes required.

**Workaround:**

You can ignore the **Advanced** button. Do not change any of the advanced options

If you add a Veritas Access cluster where the host includes the protocol (such as, https://10.20.30.40), the provider gets added and collects data but running the LTR workflow fails

Specifying the host with the protocol when you add a Veritas Access cluster is not supported in this release.

**Workaround:**

When adding a Veritas Access cluster, specify the host without protocol (such as, 10.20.30.40 instead of https://10.20.30.40).

## When you create a bucket, the status of the task appears as DONE, even though the creation is still in progress

The SDS Management Platform creates a job for creating a bucket and directly sets the status of the task as DONE. The task information is given to SDS which waits for the task to be completed.

### Workaround:

You can ignore the state of this task or job. You can find the real status in the child jobs of the `Configure Storage for Long Term Retention` job.

## Clicking on a non-mapped Veritas Access cluster directs you to an empty wiki page which shows a table and some data

A Veritas Access cluster which is discovered by the NetBackup provider and for which a Veritas Access provider is not configured may show as a link similar to the IP of the Veritas Access provider. This link may yield an empty page with some data.

### Workaround:

Add a Veritas Access provider for the cluster.

## If you restart the operating system, the SDS Management Platform does not start automatically

Currently, the SDS Management Platform is not automatically registered as a service. Hence, it is not automatically started after an operating system restart.

### Workaround:

Register the SDS Management Platform as a service using the `chkconfig --add fops` and `chkconfig fops on` commands. Or, you can start the SDS Management Platform manually using the `/etc/init.d/fops start` command.

## When you add a storage resource or backup server, the added resource is not automatically visible

When you add a storage resource or backup server, a provider is created that collects data from the Veritas Access cluster or NetBackup server respectively. This process takes some time. Therefore, the resource is not listed immediately in the table. Also, the page does not get refreshed automatically.

### Workaround:

After adding a storage resource or backup server, reload the page manually after a few minutes.

After the SDS log is rotated, the log messages from either Veritas Access or the SDS plugin go to the rotated file instead of the new file

The SDS log (located at `/var/log/sds_fops.log`) is rotated every day. SDS contains two services, the SDS plugin and the Veritas Access plugin, which share the log file. Because of bug in Python, a race condition occurs and one of the two services starts logging to a new file while the other service continues logging in the rotated file.

**Workaround:**

Check the last updated timestamps of the current log file and the rotated log file and the, co-relate the logs from different services for debugging.

Some of the storage resources may appear as faulted and a warning sign appears next to the cluster IP address in the **Infrastructure> Storage Resources** page

If you perform operations continuously on the Veritas Access cluster, then some of the storage resources may appear as faulted and a warning sign appears next to the cluster IP address in the **Infrastructure> Storage Resources** page.

**Workaround:**

There is no action required. The warning sign disappears automatically after some time.

Creation of STU fails if the S3 user is changed

After you create a bucket, if you change the S3 user, the **Create STU** operation fails.

**Workaround:**

Map the bucket with the NetBackup server using the same S3 user name for which the storage server is created.

## Software limitations

The following limitations relate to the SDS Management Platform.

- While setting the S3 parameters, the value of SSL should be set as Yes. Veritas Access supports S3 over HTTP only. Currently, Veritas Access has a limitation of not working with third-party signed certificates.
- If the S3 user is changed after bucket creation, then the **Create STU** operation fails.
- The SLP and backup policy should be already created and present on the NetBackup server.