Veritas Access Appliance Initial Configuration Guide

7.4.2 Revision 2

VERITAS™

Veritas Access Appliance Initial Configuration Guide

Last updated: 2020-02-21

Legal Notice

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.

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
Japan	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 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:

APPL.docs@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

Contents

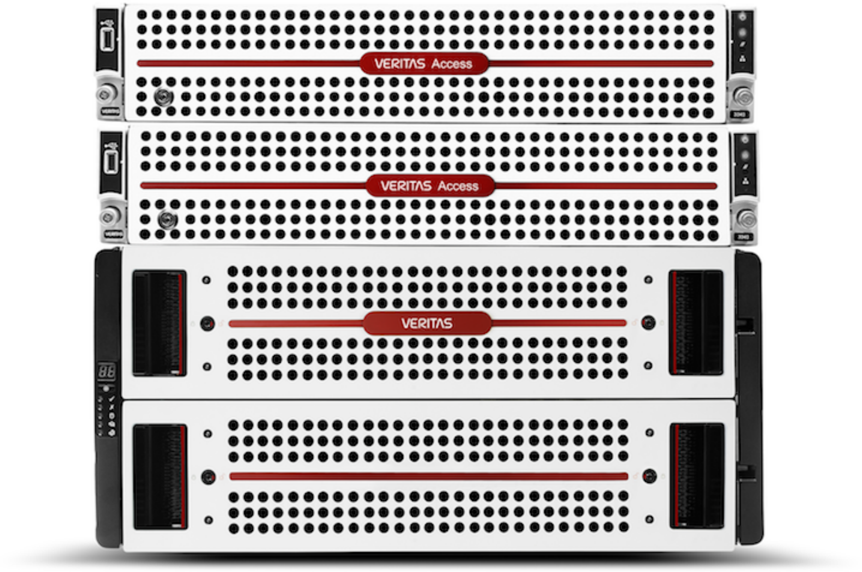
Chapter 1

Getting to know the Access Appliance

This chapter includes the following topics:

- About the Veritas Access Appliance
- About the Access Appliance administration interfaces
- About licensing the Access Appliance
- Where to find the documentation

About the Veritas Access Appliance



Veritas Access is a software-defined Network Attached Storage (NAS) solution for unstructured data. Veritas Access appliances provide a simplified and high-performing solution for deploying an Access cluster in your data center. The goal is to provide a solution that eliminates the complexities that are traditionally associated with physical server deployments.

The appliances are rack-mounted servers that run the Veritas Optimized Operating System, a Linux-based operating system. The OS, the appliance software, and the Access application come preinstalled and optimized for the server hardware and disk storage units.

The following Access appliances are available:

- Veritas Access 3340 Appliance
  For a full description of the appliance hardware, refer to the *Veritas Access 3340 Appliance Product Description*

See “About the Access Appliance administration interfaces” on page 9.

About the Access Appliance administration interfaces

The Veritas Access Appliance is administered with multiple user interfaces.

Table 1-1 Access Appliance administration interfaces

Interface	Description
Access Appliance shell menu	The Access Appliance shell menu is the interface that you use to configure, manage, and monitor the appliance-specific software and hardware of each individual node, including the attached storage. The Access Appliance shell menu is accessed locally or remotely on each node using any of the following methods: ■ SSH ■ Veritas Remote Management Console (virtual KVM) ■ Physical keyboard and monitor **Note:** The Access Appliance shell menu is available on eth1 (NIC2) once you configure the network settings during appliance initial configuration, and is also available on eth0 (NIC1) on the default IP 192.168.229.233. Common tasks to do with the Access Appliance shell menu include: ■ Initial configuration ■ Network configuration ■ Appliance user management

Table 1-1 Access Appliance administration interfaces *(continued)*

Interface	Description
Veritas Remote Management Console	The Veritas Remote Management Console provides management and monitoring capabilities independent of the appliance CPU, firmware, and operating system. This console is accessible through the Intelligent Platform Management Interface (IPMI) network port on the back of each appliance node. For the best support and initial configuration experience, Veritas recommends that you configure the IPMI port and make it accessible on your network. You can use the Veritas Remote Management Console for the following: ■ Access the Access Appliance shell menu remotely when the appliance is not accessible using regular network interfaces. ■ Manage an appliance that is turned off or unresponsive. Turn on, turn off, or restart the appliance from a remote location. ■ Monitor appliance hardware health from a remote location.
Veritas Access GUI	The Veritas Access GUI is the primary interface for Access and is used to administer the Access software on the appliance, such as creating disk pools and file systems. The Access GUI becomes available on the console IP address once the appliance cluster is configured. After the cluster configuration, the following URL is generated: http://*consoleIP*:14161/.
Veritas Access command-line interface	The Veritas Access command-line interface is used to administer the Access software on the appliance. The Access shell menu becomes available over SSH on the console IP address after the appliance cluster is configured.

For more information about the Access interfaces, refer to the *Veritas Access Administrator's Guide*.

See “Using the Access Appliance shell menu” on page 10.

See “About the Veritas Remote Management Console” on page 54.

Using the Access Appliance shell menu

The Access Appliance shell menu provides a menu-based interactive shell interface through which an administrator can manage the Veritas Access Appliance. The interface is made up of hierarchical views that contain the administrative commands and options. When you log onto the Access Appliance shell menu, the `Main_Menu` view is displayed.

```
access-cluster_01.Main_Menu>

Appliance  Access Appliance node configuration.
Exit       Logout and exit from the current shell.
Manage     Manage Access Appliance node.
Monitor    Monitor appliance activities.
Network    Network Administration.
Settings   Change appliance settings.
Shell      Shell operations.
Support    Appliance Support.
```

To navigate to sub-views or execute available commands, type the name of the option you want from the list of available options. For example, from the `Main_Menu` view, type **Manage** and press Enter to go to the `Manage` view.

Helpful tips

The following list contains some helpful tips for using the Access Appliance shell menu:

- Press Tab or Enter to auto-complete a command.
- Press the spacebar key to display the next parameter that needs to be entered.
- Type a question mark (**?**) to show more information about the commands or sub-views that are available in the current view. If you type **?** after you enter a command or option, more information about that command is shown, such as the format and usage of the command parameters.
- When you press the Enter key, the next mandatory parameter that needs to be entered is displayed. A mandatory parameter is one that does not have predefined values.

  Command parameters that are in angular brackets (*< >*) are mandatory; whereas the command parameters that are in square brackets (*[ ]*) are optional.

  For example, from the `Main_Menu > Settings > Alerts` view, the following command has one mandatory parameter and two optional parameters:

  `Email SMTP Add <Server> [Account] [Password]`

  Where *<Server>* is the mandatory SMTP server address, and *[Account]* and *[Password]* are the optional account credentials if the SMTP server requires them.
- In the Veritas Access Appliance shell menu, use the command `Return` to go back to the previous menu, and use the command `Exit` to logout and exit from

the current shell. In the Veritas Access command-line interface, use the command `Exit` to go back to the previous menu, and use the command `Logout` to logout and exit from the current shell.

See "About the Access Appliance administration interfaces" on page 9.

About licensing the Access Appliance

The Veritas Access software on the appliance includes a built-in evaluation license that activates once you complete the appliance initial configuration. This license is a trialware which can be used for 60 days. You have to obtain a perpetual license to use the Access software on the appliance after you complete the initial configuration.

To comply with the terms of the End User License Agreement, you have 60 days to obtain a valid perpetual license key. The administrator and company representatives must ensure that the appliance is entitled to the license level for the products installed. Veritas reserves the right to ensure entitlement and compliance through auditing.

For more information about the Veritas Access product licensing, refer to the *Veritas Access GUI Online Help*.

If you encounter problems while licensing this product, visit the Veritas licensing Support website.

www.veritas.com/licensing/process

The Veritas Access licensing has a few functional enforcements.

Table 1-2 Functional enforcements of Veritas Access licensing

Enforcement	Action
During Validity	None
During Grace period	Nagging message (in the GUI only)
Post Grace Period	Before you restart the node, you can stop the NFS, CIFS, FTP, and S3 services, but you cannot start the services again (even if you have not restarted the node). After you restart the node, the NFS, CIFS, FTP, and S3 services do not come ONLINE on the restarted node.

If you add the Veritas Access license using the Access GUI:

- When a node is restarted after the license has expired, the NFS, CIFS, FTP, and S3 services are stopped on that node. The status of the service appears ONLINE if the service is running anywhere in the cluster, even if it is OFFLINE on this node. Check the alerts on each node individually to see if the service is ONLINE or OFFLINE locally.
- You can start, stop, and check the status of NFS, CIFS, and S3 services. You cannot start, stop, or check the status of the FTP service.
- You can only provide the license file from the local system, the `scp` path is not supported through the GUI.

If you add the Veritas Access license using the Veritas Access shell menu:

- When a node is restarted after the license has expired, the NFS, CIFS, FTP, and S3 services are stopped on that node. You can use the `support services show` command to display the node-wise status of the service.
- You can start, stop, and check the status of NFS, CIFS, FTP, and S3 services.
- You can add the license using the `license add` command. The `license add` command provides support for `scp` path as well.
- The `license list` and `license list details` commands provide details of the license installed on each node of the cluster.

See “Configuring the Access cluster on the appliance” on page 30.

Where to find the documentation

The latest version of the Veritas Access Appliance documentation is available on the Veritas Support website and the Veritas Services and Operations Readiness Tools (SORT) website.

https://www.veritas.com/content/support/en_US/Appliances.html

https://sort.veritas.com/documents

You need to specify the product and the platform and apply other filters for finding the appropriate document.

The following guides are available for the Access Appliance:

- *Veritas Access Appliance Initial Configuration Guide*
- *Veritas Access Appliance Command Reference Guide*
- *Veritas Access 3340 Appliance Product Description*
- *Veritas Access 3340 Appliance Hardware Installation Guide*
- *Veritas Access Appliance Safety and Maintenance Guide*

- *Veritas Access Appliance Third-Party Legal Notices Guide*
- *Veritas Access Appliance Upgrade Guide*

Veritas Access documentation set

The corresponding version of the Access application documentation is available on the same page of the Veritas Services and Operations Readiness Tools (SORT) website.

The following guides are available for the Access application:

- *Veritas Access Administrator's Guide*
- *Veritas Access Command Reference Guide*
- *Veritas Access Release Notes*
- *Veritas Access RESTful API Guide*
- *Veritas Access Solutions Guide for Enterprise Vault*
- *Veritas Access Solutions Guide for NetBackup*
- *Veritas Access Troubleshooting Guide*

Preparing to configure the appliance

This chapter includes the following topics:

Initial configuration requirements

Review the information in this topic before you perform the initial configuration on the Veritas Access Appliance.

Required network addresses

Veritas Access has an advanced set of network address requirements. Review the following topic for detailed information about acquiring the necessary networking information for Access:

See "About obtaining IP addresses for Veritas Access" on page 17.

For the appliance itself, you also need to acquire the following network information:

- Two IP addresses for appliance node management over IPMI
- Two IP addresses for appliance node management over eth1
- DNS (used for Access and AutoSupport services)
- Static route and other advanced routing information
- (Recommended) IP address for the Network Time Protocol (NTP) server
- (Optional) VLAN information

- (Optional) Proxy server addresses and credentials (used for AutoSupport services)
- (Optional) SMTP or SNMP information for receiving appliance notifications and alerts

Required DNS settings

Veritas strongly recommends that you configure DNS on the appliance node. It is required to both forward and reverse DNS resolution of an FQDN (Fully Qualified Domain Name) that corresponds to the IP address assigned to eth1. A unique DNS entry is required for eth1 on each node

Without these DNS entries, the AutoSupport client cannot send out alert emails and the system health collector cannot work properly.

Configuring the host name on the appliance

You must configure a host name for an appliance node. Always use lowercase characters for the host name. The host name is applied to the appliance node and the cluster that connects with this node.

See “Configuring host name on the appliance” on page 53.

Required credentials

Two user accounts are used during initial configuration: `admin` and `maintenance`. The `admin` account is the user that logs into the appliance nodes and performs all necessary configuration steps. The `maintenance` user account performs some of the underlying processes. You are required to input the `maintenance` user's password during the appliance configuration.

Both the `admin` and `maintenance` user accounts use the same default password on new appliances:

- User name: **admin** or **maintenance**
- Password: **P@ssw0rd**

Warning: These are known default credentials to the appliance. To protect the security of the appliance, Veritas strongly recommends that you change these passwords at the designated times during the initial configuration process.

See “How to configure the Access Appliance for the first time” on page 27.

Access to the Access Appliance shell menu

Ensure that you can access the Access Appliance shell menu. All initial configuration tasks are done using this interface.

Table 2-1 Methods to access the Access Appliance shell menu

Method	Description
Veritas Remote Management Console (recommended)	You can use the Veritas Remote Management Console to launch a virtual KVM of the Access Appliance shell menu as if you were using a keyboard and mouse that are connected directly to the appliance. **Note:** You can only access the Veritas Remote Management Console if you have provisioned network access to the IPMI port on the appliance nodes (which is normally done as part of the hardware installation process). See "Configuring the IPMI port on an appliance node" on page 56.
SSH	You can use SSH for initial configuration if you have provisioned network access to the eth0 port on the appliance nodes. See "About NIC1 (eth0) port usage on the appliance nodes" on page 48.
Physical keyboard and monitor connected to the appliance	You can physically connect a standard VGA monitor and USB keyboard to the appliance node. If the appliance is powered on, the monitor displays the logon prompt for the Access Appliance shell menu.

Connectivity during initial configuration

If you configure the appliance from a remote computer, you must take precautions to avoid loss of connectivity. Any loss of connectivity during initial configuration results in failure.

Before you log onto the Access Appliance shell menu, ensure that your computer is set up to avoid the following:

- Conditions that cause the computer to go to sleep
- Conditions that cause the computer to turn off or to lose power
- Conditions that cause the computer to lose its network connection

See "Network and firewall requirements" on page 20.

About obtaining IP addresses for Veritas Access

The Veritas Access initial configuration process requires that you configure several IP addresses for the two appliance nodes.

Note: Do not use IP addresses starting with 172.16.X.X either as physical IP addresses or virtual IP addresses since this range of IP addresses are used for the private network.

Note: It is not supported to configure mixed IPv4/IPv6 addresses to any node within one cluster.

You need to obtain a contiguous range of physical IP addresses, a contiguous range of virtual IP addresses, and a netmask for the chosen public network from the network administrator in charge of the facility where the appliance is located. All IP addresses (both physical and virtual) must be part of the same subnet and use the same netmask as the node's access IP.

By design, the appliance does not support the use of the localhost (127.0.0.1) IP address during configuration.

Note: Netmask is used for IPv4 addresses. Prefix is used for IPv6 addresses. Accepted ranges for prefixes are 0-128 (integers) for IPv6 addresses.

The information you obtain from the network administrator is used to configure the following:

- Physical IP addresses
- Virtual IP addresses
- Console IP address
- IP address for the default gateway
- IP address for the Domain Name System (DNS) server
- DNS domain name

IP address requirements

Table 2-2 Required IP addresses

Number of IPs	Item
4	Physical IP addresses for public network access over eth4 and eth5
4	Virtual IP addresses for public network access over eth4 and eth5
1	IP address for the management console

Table 2-2 Required IP addresses *(continued)*

Number of IPs	Item
Total = 9	**Note:** You need four additional physical IP addresses for appliance management. See "Initial configuration requirements" on page 15.

To request and specify IP addresses

1. Request the public IP addresses that you need from your Network Administrator.
2. For example, if the Network Administrator provides you with IP addresses `10.209.105.120` through `10.209.105.123` and `10.209.105.127` through `10.209.105.131`, you can allocate the resources in the following manner:

   ```
   Start of Physical IP address: 10.209.105.120
   Start of Virtual IP address: 10.209.105.127
   Management Console IP:10.209.105.131
   ```

   This entry gives you four physical IP addresses (`10.209.105.120` to `10.209.105.123`), four virtual IP addresses (`10.209.105.127` to `10.209.105.130`), and one IP address for the Operations Manager (`10.209.105.131`).

   `10.209.105.120` and `10.209.105.121` are assigned to pubeth0 and pubeth1 as physical IP addresses on the first node.

   `10.209.105.122` and `10.209.105.123` are assigned to pubeth0 and pubeth1 as physical IP addresses on the second node.

   `10.209.105.127` to `10.209.105.130` are assigned to pubeth0 and pubeth1 as virtual IP addresses on the two nodes.

For more details about Veritas Access network requirements, refer to the *Veritas Access Installation Guide*.

See "Where to find the documentation" on page 13.

See "Network and firewall requirements" on page 20.

IP address requirements for network bonding

You can configure network bonding to group multiple network interfaces into a single logical interface. The bonded network interface increases data throughput and provides redundancy.

When you configure network bonding for public network access, bond0 is created, which groups eth4 (pubeth0) and eth5 (pubeth1) into a single logical network interface.

Use the following guidelines when you assign an IP address for the bonded network interface:

- Allocate either IPV4 public and virtual IP addresses or IPV6 public and virtual IP addresses, but not both.
- Reserve a minimum of two continuous public IP addresses for public network access.
- Reserve a minimum of two continuous virtual IP addresses for public network access.
- Reserve one virtual IP address for the Remote Management Console.

Network and firewall requirements

Ensure that your network firewall can accommodate the necessary services on the Veritas Access Appliance.

Appliance ports

In addition to the ports that are used by the Veritas Access software, the appliance also provides for both in-band and out-of-band management. The out-of-band management is through a separate network connection, the Remote Management Module (RMM), and the Intelligent Platform Management Interface (IPMI). Open these ports through the firewall as appropriate to allow access to the management services from a remote laptop or KVM (keyboard, video monitor, mouse).

Table 2-3 lists the ports open for inbound communication to the appliance.

Table 2-3 Inbound ports

Port	Service	Description
22	ssh	In-band management CLI
443	HTTPS	In-band management GUI
5900	KVM	CLI access, ISO & CDROM redirection
623	KVM	(optional, used if open)
2049	HTTPS	NFS++

Table 2-3 Inbound ports *(continued)*

Port	Service	Description
445		CIFS (for the Log/Install shares)
10082	spoold	Veritas Data Deduplication engine
10102	spad	Veritas Data Deduplication manager

* Veritas Remote Management – Remote Console

++ Once the NFS service is shut down, the vulnerability scanners do not pick up these ports as threats.

Table 2-4 lists the ports outbound from the appliance to allow alerts and notifications to the indicated servers.

Table 2-4 Outbound ports

Port	Service	Description
443	HTTPS	Call Home notifications to Veritas Download SDCS certificate
162**	SNMP	Traps sent by SNMP agents
22	SFTP	Log uploads to Veritas
25	SMTP	Email alerts
389	LDAP	
636	LDAPS	
514	rsyslog	Log forwarding
10082	spoold	Veritas Data Deduplication engine
10102	spad	Veritas Data Deduplication manager

** This port number can be changed within the appliance configuration to match the remote server.

Table 2-5 lists the out of band management ports on the appliance.

Table 2-5 Out of band management ports

80	HTTP	Out-of-band management (ISM+ or RM*)
443	HTTP	Out-of-band management (ISM+ or RM*)
5900	KVM	CLI access, ISO & CDROM redirection
623	KVM	(optional, used if open)
7578	RMM	CLI access
5120	RMM	ISO & CD-ROM redirection
5123	RMM	Floppy redirection
7582	RMM	KVM
5124	HTTPS	CDROM
5127		USB or floppy
2049	HTTPS	NFS ++
445		CIFS (for the Log/Install shares)

+ NetBackup Integrated storage manager

* Veritas Remote Management – Remote Console

++ Once the NFS service is shut down, the vulnerability scanners do not pick up these ports as threats.

Note: Ports 7578, 5120, and 5123 are for the unencrypted mode. Ports 7582, 5124, and 5127 are for the encrypted mode.

Veritas Access ports

Table 2-6 displays the default ports that Access uses to transfer information.

Table 2-6 Default Veritas Access ports

Port	Protocol or Service	Purpose	Impact if blocked
21	FTP	Port where the FTP server listens for connections. **Note:** Users can configure another port if desired.	FTP features are blocked.
22	SSH	Secure access to the Access server	Access is not accessible.
25	SMTP	Sending SMTP messages.	The SMTP messages that are sent from Access are blocked.
53	DNS queries	Communication with the DNS server	Domain name mapping fails.
111	rpcbind	RPC portmapper services	RPC services fail.
123	NTP	Communication with the NTP server	Server clocks are not synchronized across the cluster. NTP-reliant features (such as DAR) are not available.
139	CIFS	CIFS client to server communication	CIFS clients cannot access the Access cluster
161	SNMP	Sending SNMP alerts	SNMP alerts cannot be broadcast.
445	CIFS	CIFS client to server communication	CIFS clients cannot access the Access cluster.
514	syslog	Logging program messages	Syslog messages are not recorded.
756, 757, 755	statd	NFS statd port	NFS v3 protocol cannot function correctly.

Table 2-6 Default Veritas Access ports *(continued)*

Port	Protocol or Service	Purpose	Impact if blocked
2049	NFS	NFS client to server communication	NFS clients cannot access the Access cluster.
3172, 3173	ServerView	ServerView port	ServerView cannot work.
3260	iSCSI	SCSI target and initiator communication	Initiator cannot communicate with the target.
4001	mountd	NFS mount protocol	NFS clients cannot mount file systems in the Access cluster.
4045	lockd	Processes the lock requests	File locking services are not available.
5634	HTTPS	Management Server connectivity	Web GUI may not be accessible.
56987	Replication	File synchronization, Access replication	Access replication daemon is blocked. Replication cannot work.
8088	REST server	REST client to server communication	REST client cannot access REST API of Access.
8143	S3	Data port for Veritas Access S3 server	User will not able to use Veritas Access object server.
8144	ObjectAccess service	Administration port for Veritas Access S3 server.	User cannot create access or secret keys for using Objectaccess service.
11211	Memcached port	CLISH framework	CLISH cannot function correctly, and cluster configuration may get corrupted.

Table 2-6 Default Veritas Access ports *(continued)*

Port	Protocol or Service	Purpose	Impact if blocked
30000:40000	FTP	FTP passive port	FTP passive mode fails.
14161	HTTPS	Access Veritas Access GUI	User is unable to accessVeritas Access GUI
51001	UDP	LLT over RDMA	LLT is not working.
51002	UDP	LLT over RDMA	LLT is not working.

NetBackup ports

NetBackup uses TCP/IP connections to communicate between one or more TCP/IP ports. Depending on the type of operation and configuration on the environment, different ports are required to enable the connections. NetBackup has different requirements for operations such as backup, restore, and administration.

Table 2-7 shows some of the most-common TCP and UDP ports that NetBackup uses to transfer information. For more information, see the *Veritas NetBackup Security and Encryption Guide*.

Table 2-7 Default NetBackup TCP and UDP ports

Port Range	Protocol
1556	TCP, UDP
13701-13702, 13705-13706	TCP
13711, 13713, 13715-13717, 13719	TCP
13720-13722	TCP, UDP
13723	TCP
13724	TCP, UDP
13782-13783	TCP, UDP
13785	TCP

CIFS protocols and firewall ports

For the CIFS service to work properly in an Active Directory (AD) domain environment, the following protocols and firewall ports need be allowed or opened to enable the CIFS server to communicate smoothly with Active Directory Domain Controllers and Windows/CIFS clients.

Internet Control Message Protocol (ICMP) protocol must be allowed through the firewall from the CIFS server to the domain controllers. Enable "Allow incoming echo request" is required for running the CIFS service.

Table 2-8 lists additional CIFS ports and protocols.

Table 2-8 Additional CIFS ports and protocols

Port	Protocol	Purpose
53	TCP, UDP	DNS
88	TCP, UDP	Kerberos
139	TCP	DFSN, NetBIOS Session Service, NetLog
445	TCP, UDP	SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc
464	TCP, UDP	Kerberos change or set a password
3268	TCP	LDAP GC
4379	TCP	CTDB in CIFS

Table 2-9 lists the ports that are required for LDAP with SSL.

Table 2-9 LDAP with SSL ports

Port	Protocol	Purpose
636	TCP	LDAP SSL
3269	TCP	LDAP GC SSL

See “About obtaining IP addresses for Veritas Access” on page 17.

Chapter 3

Configuring the appliance for the first time

This chapter includes the following topics:

- How to configure the Access Appliance for the first time

How to configure the Access Appliance for the first time

The Veritas Access Appliance initial configuration process is broken into two phases. The first phase requires that you perform each configuration step on each individual node. You should have two terminal windows open during the first phase, each logged into one of the nodes.

During the second phase of the initial configuration, you should only perform the steps on one of the nodes. When you start the second phase of the initial configuration, close one of the terminal windows and continue doing the steps on only one of the nodes. When you initiate the cluster configuration, the settings that you configured on the current node are copied over to the second node in a one-time synchronization event.

Note: Steps that are marked as *(Recommended)* or *(Optional)* are not required to complete the initial setup of the appliance.

Table 3-1 Before you configure the Access Appliance for the first time

Step	Task
Step 1	Confirm that the appliance hardware is installed correctly and powered on. Refer to the *Veritas Access 3340 Appliance Hardware Installation Guide*.
Step 2	Review the appliance initial configuration requirements. See "Initial configuration requirements" on page 15.

First phase

For the first phase, you need to perform each step on each individual node. You should have two terminal windows open, each logged into one of the nodes.

Table 3-2 First phase of the initial configuration

Step	Task
Step 3	Log onto the Access Appliance shell menu on both nodes individually. It is helpful to have the Access Appliance shell menu of both nodes available side by side. New appliances ship with the following default login credentials: ■ User name: **admin** ■ Password: **P@ssw0rd** (where 0 is a zero) Veritas recommends that you access the shell menu using the Veritas Remote Management Console over the appliance IPMI port. See "Configuring the IPMI port on an appliance node" on page 56.
Step 4	Run the hardware self-test on each node. See "Testing the appliance hardware" on page 66.

Step 5	Check the status of each node.
	From the `Main_Menu > Appliance` view, type the following command:
	`Status`
	The appliance model, software version numbers, and node status are displayed. Both nodes should display the same software versions and the following node status:
	`Node Status: Factory installed state`

Table 3-2 First phase of the initial configuration *(continued)*

Step	Task
Step 6	Change the Maintenance user account password on both nodes. **Note:** The Maintenance user password must be the same on both nodes for the cluster configuration in the second phase to be successful. Once the cluster configuration is complete, you cannot change the Maintenance user password. See "Changing the Maintenance user account password" on page 74.
Step 7	Configure eth1 on both nodes. See "Configuring network address settings on the appliance nodes" on page 46.
Step 8	Perform a storage scan on each appliance node (one at a time) to configure the storage shelves. **Warning:** Do not start the storage scan on the second node until the first has finished. See "Scanning the storage on the appliance" on page 44.
Step 9	Configure DNS or host name mapping on both nodes. See "Configuring DNS settings on the appliance" on page 51.
Step 10	Configure the host name on both nodes. See "Configuring host name on the appliance" on page 53.

Second phase

When you start the second phase of the initial configuration, close one of the terminal windows and continue doing the steps on only one of the nodes. When you initiate the cluster configuration, the settings that you configured on the current node are copied over to the second node in a one-time synchronization event.

Table 3-3 Second phase of the initial configuration

Step	Task
Step 11 (Recommended)	Set the date and time. See "Setting the date and time on the appliance" on page 58.

Table 3-3 Second phase of the initial configuration *(continued)*

Step	Task
Step 12 (Recommended)	Configure the appliance to use a proxy server for AutoSupport and software updates. See "Setting up AutoSupport on the appliance" on page 62. See "Using a proxy server with the appliance" on page 63.
Step 13 (Recommended)	Configure the appliance to send notifications and alerts. See "Setting up email notifications on the appliance" on page 64. See "Setting up SNMP notifications on the appliance" on page 65.
Step 14	Perform the cluster configuration. See "Configuring the Access cluster on the appliance" on page 30. **Note:** During the cluster configuration, the settings that you configured on the current node are copied over to the second node in a one-time synchronization event. That means any settings you configure in the Access Appliance shell menu after the cluster configuration must be done on each node individually. The only exceptions are SMTP/SNMP and proxy server settings - these settings can sync across the nodes even after the cluster configuration.
Step 15 (Optional)	Log onto the Access GUI as `admin` to set up the Access software. When you log onto the Access GUI for the first time, you are presented with the "Veritas Access Appliance Setup" page. This wizard guides you through the necessary steps to configure the appliance for long-term retention (LTR) using Amazon S3. If you are not ready to set up LTR, you can leave this page and go to the Access dashboard. As long as LTR is not configured, the Getting Started progress is displayed at the top of the dashboard and you can return to it at any time.

See "Where to find the documentation" on page 13.

Configuring the Access cluster on the appliance

This procedure configures the Veritas Access cluster on the appliance. This procedure is only performed during the initial configuration of the appliance. Ensure that you complete all of the other necessary steps in the initial configuration process before you configure the cluster.

See "How to configure the Access Appliance for the first time" on page 27.

To configure the Veritas Access cluster on the appliance

1. Log on to the Access Appliance shell menu of one of the appliance nodes.

2. From the `Main_Menu > Manage > Cluster` view, type the following command to start the cluster configuration wizard:

   ```
   Configure
   ```

3. Type **yes** to continue.

4. Enter a name for the cluster.

   Cluster names should be DNS-compatible. DNS-compliant cluster names should conform to the following naming conventions:

   - Must be at least three and no more than 10 characters long.
   - Allowed characters in a cluster name are lowercase letters, numbers, and hyphens ‘a-z, 0-9, -‘. Any other character is invalid.
   - Must start with a lowercase letter and must not start with a hyphen ('-') or number.
   - Must end with a lowercase letter or a number.
   - Should not be an IP address.

5. Enter the eth1 IP addresses for each node, separated by a space.

6. Type the password of the Maintenance user of both nodes.

   Note: The Maintenance user password must be the same on each node or the configuration fails. To protect the security of the appliance, you should change the Maintenance user password of each node before you start the cluster configuration. You cannot change the Maintenance user password after the cluster is configured.

7. Specify whether you want to configure network bonding for the public network interfaces eth4 and eth5. To configure network bonding, type **yes** and continue to step 8; else type **no** and go to step 9.

   Note: Network bonding can be configured only when you configure the cluster.

8. If you typed **yes** in step 7, complete the following steps and go to step 11.

   - Specify the mode for the network bonding.

- If you select mode 3 (balance-xor) or 5 (802.3ad), specify the transmit hash policy to use.
- Enter the starting IP address from the range of public IP addresses that you had reserved. At a minimum, you need to reserve two continuous public IP addresses.
- Enter the starting virtual IP address from the range of virtual IP addresses that you had reserved. At a minimum, you need to reserve two continuous virtual IP addresses.

See “About obtaining IP addresses for Veritas Access” on page 17.

9 Enter the starting IP address of the four public IP addresses that you have reserved.

For example, if you type `10.182.12.89`, the appliance will use 10.182.12.89-92 for public IP addresses.

See “About obtaining IP addresses for Veritas Access” on page 17.

10 Enter the starting IP address of the four virtual IP addresses that you have reserved.

11 Enter the netmask for the public IP addresses.

12 Enter the default gateway IP address.

13 Enter the DNS server IP address.

14 Enter the DNS server domain name.

15 Enter the console virtual IP address.

16 Review the configuration summary and type **yes** to continue and begin the configuration.

If you have configured network bonding, bond0 is created for the public network and the message **Public network connection provided by bond0 with subordinate network interfaces** is displayed.

The configuration process can take around 40 minutes to complete.

17 You are prompted to change the password of the admin user account. Type **yes** to change it.

Veritas recommends that you change the admin user account's password since it is a known default password. If you do not change this account's password now, you must do it later in the Access shell menu.

18 After the cluster is configured, you are prompted to reboot the cluster to bring up the Access services. Type **yes**.

Note: If you choose to reboot the cluster later, you can access the cluster but all the functionality might not be supported till all the services are up.

After the configuration is complete, you can log into all of the user interfaces on the appliance.

Table 3-4 Appliance user interface addresses

Interface	IP address
Access Appliance shell menu for node 1	Node 1 eth1 IP over SSH
Access Appliance shell menu for node 2	Node 2 eth1 IP over SSH
Access shell menu	Console IP over SSH
Access GUI	http://*consoleIP*:14161/

See “About the Access Appliance administration interfaces” on page 9.

Chapter 4

Getting started with the Veritas Access GUI

This chapter includes the following topics:

- Where to find the Veritas Access GUI
- About the Veritas Access 3340 Appliance

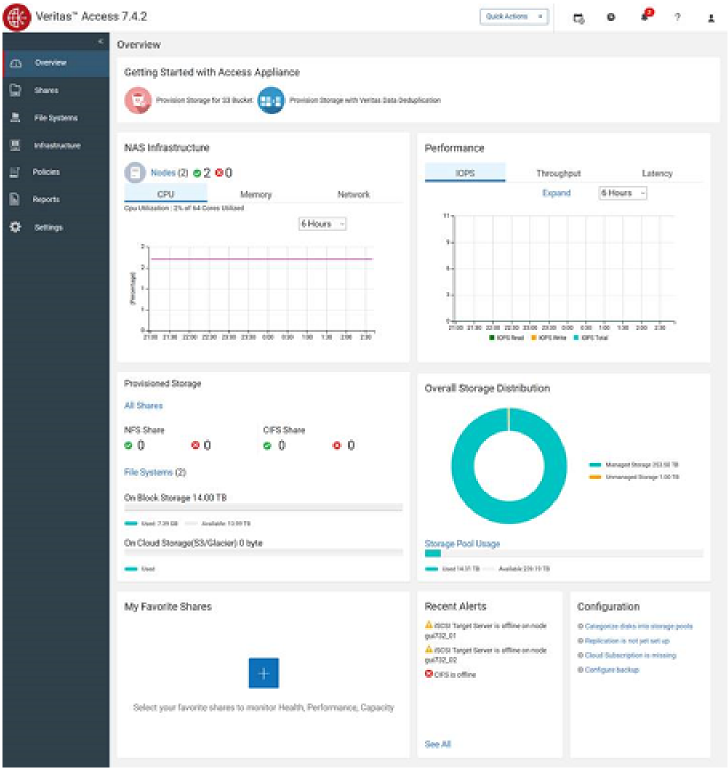
Where to find the Veritas Access GUI

The Veritas Access GUI is automatically installed with the Veritas Access installer.

After the installation, the following URL is generated: http://*consoleIP*:14161/.

The URL for accessing the GUI is displayed after logging on to the Veritas Access CLI.

Open a browser window and copy in the generated URL to access the GUI. See the online Help for information on all the GUI operations. Click ? to access the online Help.



⚠ iSCSI Target Server is offline on node gui732_01

⚠ iSCSI Target Server is offline on node gui732_02

CIFS is offline

About the Veritas Access 3340 Appliance

Veritas Access in an appliance form factor provides a cost-effective, performant, scalable, and highly available storage for storing data and retaining it for the compliance policies. You can use the Veritas Access 3340 Appliance for long-term retention (LTR) of backup images.

Note: The Veritas Access 7.4.2 release is a standalone release as well as an appliance-oriented release. You can find all the documents related to the Veritas Access 3340 Appliance on the SORT site:

Installation and Configuration - https://sort.veritas.com/documents/doc_details/AAPP/7.4.2/Appliance%203340/InstallationandConfiguration/

Product Guides - https://sort.veritas.com/documents/doc_details/AAPP/7.4.2/Appliance%203340/ProductGuides/

Supplemental Content - https://sort.veritas.com/documents/doc_details/AAPP/7.4.2/Appliance%203340/SupplementalContent/

You can set up the Veritas Access 3340 Appliance by provisioning storage for:

- Veritas Data Deduplication
  Veritas recommends using Veritas Data Deduplication for long-term retention of data rather than using the long-term data retention (LTR) solution.
- S3 Bucket

Note: It is recommended to use only the LTR policies on the Veritas Access 3340 Appliance. All non-LTR policies use striped-mirror or mirror, which is not recommended on the Veritas Access 3340 Appliance because it already uses RAID-6 to protect the data. If you use other than LTR policies, it may result in consumption of twice of the capacity to store the same amount of data. To avoid it, you can manually select a file system to create a basic file system in the Veritas Access GUI instead of a policy, or use the Access command-line interface for full access to all the options for all the use cases. The use cases include adding replication, configuring a scale-out file system, and so on. The LTR policies use **Simple** as the default file system type. To view it, in the Veritas Access GUI, you can go to **Settings** > **S3 Management** > **Default parameters for S3 buckets** > **File system type**.

See “Configuring Veritas Data Deduplication” on page 37.

See “Configuring storage for LTR” on page 41.

Configuring Veritas Data Deduplication

To configure Veritas Data Deduplication

1. Log on to the **Veritas Access** application.

   The **Getting Started with Access Appliance** page is displayed.

2. Click **Provision Storage with Veritas Data Deduplication**.

   By default, the **Configure Storage** tab is displayed.

3. Create a storage pool, modify disk selections for the pool as required, and then click **Configure Storage**.

   By default, all the available disks are selected for the pool.

   When you create a Veritas Data Deduplication storage pool, you need to use five disks or volumes. You add disks or volumes in multiples of five.

4. Under the **Activate Policy** tab, select the Veritas Data Deduplication policy, and then click **Activate Policy**.

5. Click **Next**.

6. Specify the storage options, enter the user name and password for the service, enter a virtual IP for the service, and then click **Provision Storage**.

   You can use:

   - The virtual IP address to connect to the Data Deduplication server.
     Use the Access command-line interface `Network> ipaddress show` command to find the virtual IP address.
     In the Veritas Access GUI, navigate to **NAS Infrastructure > Nodes**, and click on the node name to see the virtual IP address.
   - The user name and password to log on to the Veritas Data Deduplication server.
     The password needs to be the same as the password you used to configure and add the storage unit on NetBackup.

7. View the **Recent Activity** panel for the status of the task.

See “Unconfiguring Veritas Data Deduplication” on page 40.

See “About Veritas Data Deduplication” on page 38.

See “Viewing information about Veritas Data Deduplication” on page 39.

See “Starting or stopping the Veritas Data Deduplication service” on page 40.

See “Increasing storage for Veritas Data Deduplication” on page 39.

About Veritas Data Deduplication

Veritas Access is integrated with a duplication engine which is based on Media Server Deduplication Pool (MSDP) technology for storing backup data. The storage server component of Veritas Data Deduplication runs on the Veritas Access nodes with high availability in active/passive mode. The deduplication plug-in of the NetBackup media server does segmentation and finger printing of the backup data and sends the deduplicated data to Veritas Access. The Veritas Data Deduplication storage server stores and manages the deduplicated data. The deduplication storage server provides high availability to protect against storage, node, and network failures. It supports client direct as well as media server deduplication configurations.

All storage that is provisioned for Veritas Data Deduplication is displayed as a single storage pool on NetBackup.

Note: The Veritas Data Deduplication feature is not supported on the Oracle Linux platform.

Note: To use the Veritas Data Deduplication service, you need to get an add-on license. The deduplication functionality is licensed separately and is generated based on your requirement.

See “Add-on license for using Veritas Data Deduplication” on page 38.

See “Configuring Veritas Data Deduplication” on page 37.

See “Starting or stopping the Veritas Data Deduplication service” on page 40.

See “Increasing storage for Veritas Data Deduplication” on page 39.

See “Unconfiguring Veritas Data Deduplication” on page 40.

See “Viewing information about Veritas Data Deduplication” on page 39.

Add-on license for using Veritas Data Deduplication

In addition to the base license, you can also procure an add-on license to use the Veritas Data Deduplication service. The deduplication functionality is licensed separately and is generated based on your requirement. The add-on deduplication license is applied when the base license key is present and is associated with both capacity and time period. The validity of the add-on license may be different from the base license.

The add-on license can also be purchased together with the base Veritas Access license. The new license includes the base license (Per-TB) along with the deduplication license.

If you already have a valid Veritas Access license, and you want to upgrade to Veritas Access 7.4.2, you can procure the add-on deduplication license, or you can purchase the combined license with the Per-TB license along with deduplication.

You can install your license key using the Veritas Access command-line interface or the Veritas Access GUI.

Note: Even if you have installed the add-on deduplication license, the licensing reports display only the base licensing information. All the functionalities are also with respect to the base key only.

If you have installed either the add-on deduplication license or the combined base license with deduplication, you can see the information on the deduplication license using the following command that displays all the valid licenses installed on your system.

```
/sbin/slic/vxlicrep
```

Viewing information about Veritas Data Deduplication

From the **Settings > Veritas Data Deduplication** page, you can view the service details for Veritas Data Deduplication.

You can modify the service status and unconfigure Veritas Data Deduplication.

Under **Service Details**, you can view the following:

- File system name
- Virtual IP address
- Service status

See “About Veritas Data Deduplication” on page 38.

See “Starting or stopping the Veritas Data Deduplication service” on page 40.

See “Increasing storage for Veritas Data Deduplication” on page 39.

See “Unconfiguring Veritas Data Deduplication” on page 40.

See “Configuring Veritas Data Deduplication” on page 37.

Increasing storage for Veritas Data Deduplication

You can increase storage for Veritas Data Deduplication.

To increase storage for Veritas Data Deduplication

1. Go to **Settings > Veritas Data Deduplication**.
2. Under **Deduplication Storage**, click **Grow Storage**.

   The **Grow Veritas Data Deduplication Storage** dialog box is displayed.
3. Specify the storage options for Veritas Data Deduplication and confirm the settings.

   When you grow a Veritas Data Deduplication storage pool, you need to use five disks or volumes. You add disks or volumes in multiples of five.
4. View the **Recent Activity** panel for the status of the task.

See “About Veritas Data Deduplication” on page 38.

See “Viewing information about Veritas Data Deduplication” on page 39.

See “Starting or stopping the Veritas Data Deduplication service” on page 40.

See “Configuring Veritas Data Deduplication” on page 37.

See “Unconfiguring Veritas Data Deduplication” on page 40.

Starting or stopping the Veritas Data Deduplication service

You can start or stop the Veritas Data Deduplication service.

To start or stop the Veritas Data Deduplication service

1. Go to **Settings > Veritas Data Deduplication > Deduplication Details > Service Status**, and click the circle to stop or start the service.
2. Confirm that you want to start or stop theVeritas Data Deduplication service.
3. View the **Recent Activity** panel for the status of the task.

See “About Veritas Data Deduplication” on page 38.

See “Viewing information about Veritas Data Deduplication” on page 39.

See “Increasing storage for Veritas Data Deduplication” on page 39.

See “Unconfiguring Veritas Data Deduplication” on page 40.

See “Configuring Veritas Data Deduplication” on page 37.

Unconfiguring Veritas Data Deduplication

You can unconfigure Veritas Data Deduplication.

To unconfigure Veritas Data Deduplication

1. Go to **Settings > Veritas Data Deduplication**.
2. Under **Deduplication Details**, click **Unconfigure**.

   The **Unconfigure Veritas Data Deduplication** dialog box is displayed.
3. Confirm the settings and click **OK**.
4. View the **Recent Activity** panel for the status of the task.

See “Configuring Veritas Data Deduplication” on page 37.

See “About Veritas Data Deduplication” on page 38.

See “Viewing information about Veritas Data Deduplication” on page 39.

See “Starting or stopping the Veritas Data Deduplication service” on page 40.

See “Increasing storage for Veritas Data Deduplication” on page 39.

Configuring storage for LTR

You can configure storage for LTR.

To configure the storage

1. Log on to the **Veritas Access** application.

   The **Getting Started with Access Appliance** page is displayed.
2. Click **Provision Storage for S3 Bucket**.

   By default, the **Configure Storage** tab is displayed.
3. Specify the storage options, and then click **Configure Storage**.

   Note: By default, a file system of 1 GB is created and all disks from the infrastructure are selected. You can modify the disk selection for the file system.
4. Click the **Configure S3 Server** tab, specify a pool, enable or disable SSL, and then click **Configure S3**.
5. Click the **Activate LTR Policy** tab, select a pool or pool(s), and then click **Activate Policy** to activate an LTR policy.

   Note: For the Veritas Access 3340 Appliance, only an LTR on-premises policy is supported.

6. Click the **Generate S3 Keys** tab, type your user name and password, and then click **Generate Keys**.
7. Click the **Provision Storage** tab, enter a bucket size, type the access and the secret keys, and then click **Provision Storage**.
8. Click **View Details** or **Recent Activity** to view the status of the activity.

Chapter 5

Storage management

This chapter includes the following topics:

- About the appliance storage
- Viewing the storage on the appliance
- Scanning the storage on the appliance

About the appliance storage

The Veritas Access 3340 Appliance must be connected to one Primary Storage Shelf. The storage space can be expanded by using up to three Expansion Storage Shelves. After you have physically connected the storage shelves, use the Access Appliance shell menu to discover and refresh the storage devices information. All the appliance nodes share the external storage that is attached to the appliance.

Note: The Veritas Access 3340 compute nodes do not have internal disk space available for Access storage. Only the space available on the Primary Storage Shelf and Expansion Storage Shelves can be used for Access data.

The physical disk storage in the Primary Storage Shelf contains five Data volumes, five Fencing volumes, and one Configuration volume.

The physical disk storage in the Expansion Storage Shelf contains five Data volumes.

The Data, Fencing, and Configuration volumes are created when you scan the storage that is attached to the appliance. The Access software only uses the Data volumes to provision storage.

See “Scanning the storage on the appliance” on page 44.

See “Viewing the storage on the appliance” on page 44.

Viewing the storage on the appliance

After you scan the appliance storage, you can use the `Manage > Storage > Show Disk` command to view storage details.

To view appliance storage information

1. Log on to the Access Appliance shell menu on an appliance node.
2. Go to the `Manage > Storage` view.
3. Run the `Show Disk` command.

The disks that are listed by the `Show` command are not the physical disks themselves. Rather, they are storage volumes that are made up of specific physical disks in the storage shelf.

Table 5-1 Disk (volume) types

Type	Description
System	The onboard storage that is occupied by the appliance operating system, logs etc. This disk is located in the compute node, and not in the storage shelf.
Configuration	This volume stores the configuration information. The disk is always located in the Primary Storage Shelf.
Data	The Access software uses the Data volumes to provision storage. There are five data disks in the Primary Storage Shelf or each of the Expansion Storage Shelves.
Fencing	There are five Fencing volumes in the Primary Storage Shelf. The Fencing volumes do not exist in the Expansion Storage Shelves.
Unknown	This category appears when the appliance cannot determine the disk type, such as when the disk is not accessible.

See “Scanning the storage on the appliance” on page 44.

See “About the appliance storage” on page 43.

Scanning the storage on the appliance

Use this command to scan the storage from each node (one at a time) for the appliance.

Warning: Do not start the storage scan on the second node until the first has finished.

See “How to configure the Access Appliance for the first time” on page 27.

Note: If the appliance has been re-imaged, you must perform a storage reset before you can perform this procedure.

To scan the appliance storage

1. Log on to the Access Appliance shell menu of one of the appliance nodes.
2. From the `Main_Menu > Manage > Storage` view, type the following command to scan the storage:

   ```
   Scan
   ```

   Wait for the `Scan` operation to complete on the current node.
3. Repeat this procedure on the other node.

See “Viewing the storage on the appliance” on page 44.

Chapter 6

Network connection management

This chapter includes the following topics:

- Configuring network address settings on the appliance nodes
- About VLAN tagging on the appliance
- Configuring static routes on the appliance
- Configuring DNS settings on the appliance
- Configuring host name on the appliance
- About the maximum transmission unit size on the appliance
- About the Veritas Remote Management Console
- Setting the date and time on the appliance

Configuring network address settings on the appliance nodes

You can configure the network settings for eth0 and eth1 of an appliance node.

Note: Review IPv4-IPv6 support information before you begin.

See "About IPv4-IPv6-based network support on the Access Appliance" on page 49.

To configure the appliance node to communicate with one network

1. Log on to the Access Appliance shell menu on the desired node.
2. From the `Main_Menu > Network` view, type the following command to verify which network ports and bonds are plugged and available for configuration:

   ```
   Show Status
   ```

3. Type the following command to configure the appliance to connect to a single network:

   ```
   Configure <IPAddress> <Netmask> <GatewayIPAddress>
   <InterfaceNames>
   ```

   - *<IPAddress>* - The new IP address that you want to assign to the network interface.
   - *<Netmask>* - The subnet mask (IPv4) or prefix length (IPv6).
   - *<GatewayIPAddress>* - The default gateway for the appliance node.
   - *<InterfaceNames>* - The network port that you want to assign the configuration to, such as `eth1`.

   For example:

   ```
   Configure 10.182.20.255 255.255.224.0 10.182.1.1 eth1
   ```

   Note: You should not use both IPv4 and IPv6 addresses in the same command, such as the following:

   ```
   Configure 9ffe::9 255.255.255.0 1.1.1.1
   ```

To configure the appliance node to communicate with more than one network

1. Log on to the Access Appliance shell menu on the current node.
2. From the `Main_Menu > Network` view, type the following command to verify which network ports are available for configuration:

   ```
   Show Status
   ```

3. Type the following command to configure an IPv4 address for the network interface:

   ```
   IPv4 <IPAddress> <NetMask> <InterfaceNames>
   ```

   ```
   IPv6 <IPAddress> <Prefix> <InterfaceNames>
   ```

   - *<IPAddress>* - The new IPv4 or IPv6 address that you want to assign to the network interface.

- *<Netmask>* and *<Prefix>* - The subnet mask (IPv4) or prefix length (IPv6).
- *<InterfaceName>* - The network interface that you want to assign the configuration to, such as `eth1` .

For example:

```
Configure 9ffe::46 64 9ffe::49 eth1
```

4 (Optional) If you are configuring the appliance for the first time, you need to configure a default gateway for the appliance. You can then specify a gateway for each specific network configuration, if desired.

Type the following command:

```
Gateway Add <GatewayIPAddress> [TargetNetworkIPAddress] [Netmask]
[InterfaceName]
```

- *<GatewayIPAddress>* - The IP address leading to the remote network (generally a gateway or router).
- *[TargetNetworkIPAddress]* - The IP address of the destination network or host.
- *[Netmask]* - The subnet mask (IPv4) or prefix length (IPv6) that corresponds to the address that you specified for *[TargetNetworkIPAddress]*.
- *[InterfaceName]* - The name of the network interface that you want the traffic to exit from.

For example:

```
Gateway Add 192.168.1.1 10.10.0.0 255.255.248.0 eth1
```

See “Configuring network address settings on the appliance nodes” on page 46.

See “About NIC1 (eth0) port usage on the appliance nodes” on page 48.

See “About the maximum transmission unit size on the appliance” on page 53.

About NIC1 (eth0) port usage on the appliance nodes

By default, NIC1 (eth0) is set to IP address 192.168.229.233. This private network address is reserved to provide a direct connection from a laptop to perform the initial configuration. NIC1 (eth0) is typically not connected to your network environment.

If after initial configuration you want to repurpose NIC1 (eth0), you can change the IP address using the `Network > IPv4` or `Network > IPv6` commands.

Note: If another appliance network interface is set to the 192.168.x.x IP address range, you must change the default IP address of NIC1 (eth0) to a different IP address range.

See "Configuring network address settings on the appliance nodes" on page 46.

About IPv4-IPv6-based network support on the Access Appliance

Note: This topic only applies to eth0 and eth1 of the appliance nodes. These ports are used for appliance management and not for the Veritas Access software. You can only configure IPv4 addresses for Veritas Access.

The Veritas Access Appliance supports a dual stack IPv4-IPv6 network. You can assign an IPv6 address to an appliance, configure DNS, and configure routing to include IPv6 based systems.

Consider the following points for IPv6 addresses:

- The appliance does not support a pure IPv6 network. An IPv4 address must be configured for the appliance node management interface (eth1), otherwise the initial configuration which requires the appliance nodes' management IP addresses is not successful.
- Only global addresses can be used, not addresses with link-local or node-local scope. Global-scope and unique-local addresses are both treated as global addresses by the host.
  Global-scope IP addresses refer to the addresses that are globally routable. Unique-local addresses are treated as global.
- You cannot use both an IPv4 and an IPv6 address in the same command. For example, you cannot use `Configure 9ffe::9 255.255.255.0 1.1.1.1`. You should use `Configure 9ffe::46 64 9ffe::49`.
- Embedding the IPv4 address within an IPv6 address is not supported. For example, you cannot use an address like `9ffe::10.23.1.5`.
- You can enter only one IPv4 address for a network interface card (NIC). However, you can enter multiple IPv6 addresses for a NIC.
- Network File System (NFS) or Common Internet File System (CIFS) protocols are supported over an IPv4 network on the appliance. NFS or CIFS are not supported on IPv6 networks.
- The `Main_Menu > Network > Hosts` command supports multiple IPv6 addresses to be assigned to the same host name having one network interface card (NIC).

However, only one IPv4 address can be assigned to a specific host name having one NIC using this command.

- You can add an IPv6 address of a network interface without specifying a gateway address.

See “Configuring network address settings on the appliance nodes” on page 46.

About VLAN tagging on the appliance

You can assign a VLAN ID to an appliance-managed network interface (eth0 or eth1) after the appliance is configured and the Access cluster is running

Note: After the appliance is configured and the Access cluster is running, eth0 and eth1 are the only available network interfaces for VLAN tagging from the Access Appliance shell menu.

For how to assign a VLAN ID to an Access-managed network interface, refer to the *Veritas Access Administrator’s Guide*.

Use the following guidelines when assigning a VLAN ID:

- The selected network interface must be plugged.
- The selected interface cannot have an IP address assigned to it.
  If an IP address is assigned to the selected interface, you must first remove that IP address before you attempt to assign a VLAN ID.

To assign a VLAN tag

1. Log on to the Access Appliance shell menu.
2. From the `Main_Menu > Network` view, type the following command:

   ```
   VLAN Tag <VLANID> <InterfaceName> [IPAddress] [Netmask]
   ```

   Where <*VLANID*> is the VLAN identifier (1 - 4094) and <*InterfaceName*> is the name of the interface to which you want to assign the VLAN tag. The *[[IPAddress]]* parameter can be an IPv4 or an IPv6 address and the *[[Netmask]]* parameter is the netmask (IPv4) or prefix length (IPv6).

See “Configuring network address settings on the appliance nodes” on page 46.

Configuring static routes on the appliance

You can configure static routes on an appliance node to communicate with remote networks or hosts if the default route is not suitable. You can also use static routes to filter traffic to specific network interfaces, or to create a backup routing configuration in case the default gateway fails.

For more information about static routes, refer to the following documentation:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sec-Configuring_Static_Routes_in_ifcfg_files.html

To add a static route

1 Log on to the Access Appliance shell menu on an appliance node.

2 From the `Main_Menu > Network` view, type the following command:

```
Gateway Add <GatewayIPAddress> [TargetNetworkIPAddress] [Netmask]
[InterfaceName]
```

- *<GatewayIPAddress>* - The IP address leading to the remote network (generally a gateway or router).
- *[TargetNetworkIPAddress]* - The IP address of the destination network or host.
- *[Netmask]* - The subnet mask that corresponds to the address that you specified for *[TargetNetworkIPAddress]*.
- *[InterfaceName]* - The name of the network interface that you want the traffic to exit from.

For example:

```
Gateway Add 192.168.1.1 10.10.0.0 255.255.248.0 eth1
```

3 Repeat this procedure on the other node.

See “Configuring network address settings on the appliance nodes” on page 46.

Configuring DNS settings on the appliance

Veritas strongly recommends that you configure DNS on the appliance node. It is required for both forward and reverse DNS resolution of an FQDN (Fully Qualified Domain Name) that corresponds to the IP address assigned to eth1.

See “Initial configuration requirements” on page 15.

Note: Make sure that the network names of all appliances are DNS resolvable (FQDN and short name).

Note: Make sure that forward and reverse DNS lookups are configured properly in your environment. If a forward or a reverse DNS lookup returns multiple records, the initial configuration may fail. You can check the DNS configuration with the following commands for each node. Each command should return only one entry

Linux:

```
dig +short @<DNS server IP address> a <node hostname>
dig +short @<DNS server IP address> -x <node IP address>
```

Windows:

```
nslookup <node IP address>
nslookup <node hostname>
```

To configure DNS settings

1. Log on to the Access Appliance shell menu on one of the appliance nodes.
2. From the `Main_Menu > Network` view, type the following command to add a DNS name server:

   ```
   DNS Add NameServer <IPAddress>
   ```

   Where <*IPAddress*> is the IP address of the name server. You can add multiple name servers.
3. Type the following command to add a DNS search domain:

   ```
   DNS Add SearchDomain <DomainName>
   ```

   Where <*DomainName*> is the target domain for searching. For example:

   ```
   DNS Add SearchDomain mn.us.company.com
   ```

   You can add multiple search domains.
4. Type the following command to configure the DNS domain name suffix:

   ```
   DNS Domain <Name>
   ```

   Where <*Name*> is the domain name of the DNS server. For example:

   ```
   DNS Domain mn.us.company.com
   ```

5. Repeat this procedure on the other node.

To manually add an IP address and host name mapping

1 Log on to the Access Appliance shell menu on one of the appliance nodes.

2 From the `Main_Menu > Network` view, type the following command to manually add a host name:

```
Hosts Add <IPAddress> <FQHN> <ShortName>
```

Where <*IPAddress*>, <*FQHN*>, and <*ShortName*> are the IP address, fully qualified host name, and the short host name of the host.

3 Repeat this procedure on the other node.

See “About IPv4-IPv6-based network support on the Access Appliance” on page 49.

Configuring host name on the appliance

You must configure a host name for any appliance node. The naming convention for a host name is to use lowercase letters. The host name is applied to the appliance node and the cluster that connects with this node.

Note: Do not configure the same host name to two appliance nodes that connect to a same cluster.

To configure the host name on your appliance node

1 Log on to the Access Appliance shell menu on one of the appliance nodes.

2 From the `Main_Menu > Network` view, type the following command to configure a host name:

```
Hostname Set <Name>
```

Where <*Name*> is the short host name or the fully qualified domain name (FQDN) of the appliance node.

About the maximum transmission unit size on the appliance

The MTU property controls the maximum transmission unit size for an ethernet frame. The standard maximum transmission unit size for Ethernet is 1500 bytes (without headers). In supported environments, the MTU property can be set to larger values in excess of 9,000 bytes. Setting a larger frame size on an interface is commonly referred to as using jumbo frames. Jumbo frames help reduce fragmentation as data is sent over the network and in some cases, can also provide better throughput and reduced CPU usage. To take advantage of jumbo frames, the Ethernet cards, drivers, and switching must all support jumbo frames. Additionally, each server interface that is used to transfer data to the appliance must be configured for jumbo frames.

Veritas recommends that if you configure the MTU property of an interface to values larger than 1500 bytes, make sure that all systems that are connected to the appliance on the specific interface have the same maximum transmission unit size. Such systems include things as remote desktops. Also verify the network hardware, OS, and driver support on all systems before you configure the MTU property.

You can configure the MTU property of an appliance network interface using the `SetProperty` command from `Main > Network` view of the Access Appliance shell menu.

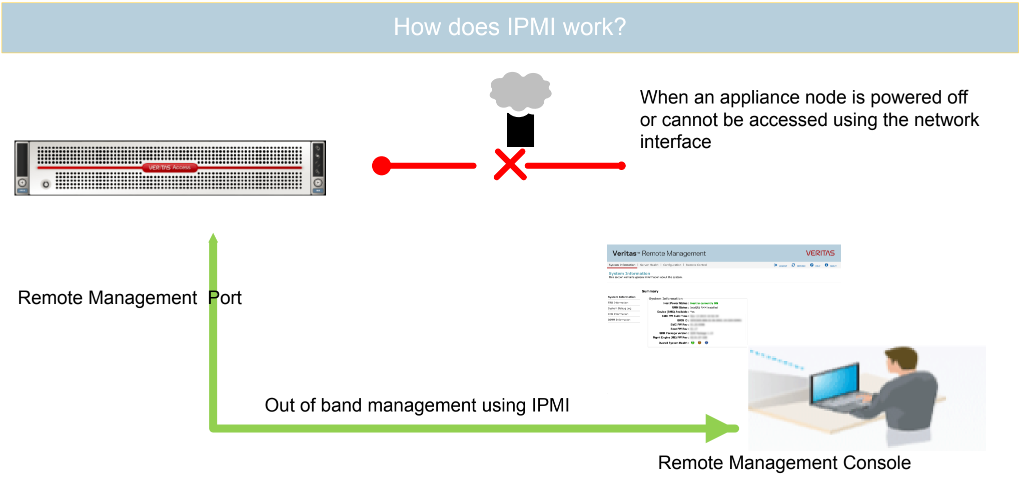
See “Configuring network address settings on the appliance nodes” on page 46.

About the Veritas Remote Management Console

The Veritas Remote Management Console provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system. This console is accessible through the Intelligent Platform Management Interface (IPMI) network port on the back of each appliance node. For the best support and initial configuration experience, Veritas recommends that you configure the IPMI port and make it accessible on your network.

The Veritas Remote Management Console is beneficial after an unexpected power outage shuts down the connected system. In case the appliance node is not accessible after the power is restored, you can use a PC to access the appliance node remotely by using a network connection to the hardware rather than to an operating system or login shell. The Veritas Remote Management Console enables you to control and monitor the appliance node even if it is powered off, unresponsive, or without any operating system.

Figure 6-1 Diagram of how IPMI works


How does IPMI work?
When an appliance node is powered off or cannot be accessed using the network interface
VERITAS Access
Remote Management Port
Veritas Remote Management
VERITAS
Out of band management using IPMI
Remote Management Console

You can use the Veritas Remote Management Console for the following:

- Manage an appliance node that is turned off or unresponsive. Turn on, turn off, or restart the appliance node from a remote location.
- Provides out-of-band management and helps manage situations where local physical access to the appliance is not possible or preferred, like branch offices and remote data centers.
- Access the Access Appliance shell menu remotely when the appliance is not accessible using regular network interfaces.
- Reimage the appliance node using ISO redirection.
- Monitor appliance node hardware health from a remote location.
- Avoid messy cabling and hardware like keyboard, monitor, and mouse (KVM) solutions.

Supported browsers

- Microsoft Edge
- Mozilla Firefox 46.x and newer
- Google Chrome 50.x and newer
- Apple Safari 9.x and newer

Configuring the IPMI port on an appliance node

To configure the IPMI port using the Access Appliance shell menu

1. To configure the IPMI locally, connect the following components to the appropriate ports on the rear panel of the appliance node:

   - A standard video cable between the VGA (Video Graphics Array) port and a computer monitor.
   - A USB keyboard to a USB port on the appliance node.

   To configure the IPMI remotely over the network, use SSH to connect to the appliance node management IP on eth0.

2. Log on to the Access Appliance shell menu.

   Enter the user name and password for the appliance node. By default, the user name is `admin` and the password is `P@ssw0rd` where 0 is the number zero.

3. Go to the `Main_Menu > Support` view.

4. Enter the following command to configure the IPMI port:

   ```
   IPMI Network Configure <IPAddress> <Netmask> <GatewayIPAddress>
   ```

   Where *IP address* is the new IP address for the IPMI port. The Subnet mask and Gateway enable connectivity between your network computer and the IPMI port.

   The IPMI port must be configured as a DHCP or static address.

   At any point in time, you can run the following command to see the IPMI network details:

   ```
   IPMI Network Show
   ```

5. Type `Exit` and press Enter to log out of the Access Appliance shell menu.

6. If you have already connected the IPMI port to your network with a Cat5 ethernet cable, check that you can reach the Veritas Remote Management Console using the new address in a web browser.

See “Resetting the IPMI on an appliance node” on page 58.

See “Managing IPMI users on an appliance node” on page 56.

Managing IPMI users on an appliance node

The following procedures use the Access Appliance shell menu. You may be able to perform the same tasks from the Veritas Remote Management Console.

To add a Veritas Remote Management Console user

1. Log on to the Access Appliance shell menu.
2. Run the following command:

   ```
   Support > IPMI User Add <user_name>
   ```

   Where <*user_name*> is the new user that you want to add.
3. When prompted, enter and confirm a password for the new user:

   ```
   access-appl.Support> IPMI User Add abc
   New password: <password>
   Confirm password: <password>
   Operation successful
   ```

To view the Veritas Remote Management Console users

1. Log on to the Access Appliance shell menu.
2. Run the following command:

   ```
   Support > IPMI User List
   ```

   ```
   vel-appl.Support > IPMI User List
   User name          : abc
   User privilege     : ADMIN

   User name          : sysadmin
   User privilege     : ADMIN

   User name          : root
   User privilege     : ADMIN
   ```

To delete a Veritas Remote Management Console user

1. Log on to the Access Appliance shell menu.
2. Run the following command:

   ```
   Support > IPMI User Delete <user_name>
   ```

   Where <*user_name*> is an existing user that you want to delete.

   ```
   access-appl.Support> IPMI User Delete abc
   User abc has been deleted successfully.
   ```

See “Resetting the IPMI on an appliance node” on page 58.

See “Configuring the IPMI port on an appliance node” on page 56.

Resetting the IPMI on an appliance node

If the Veritas Remote Management Console stops responding, you can reset it using the `Support > IPMI Reset` command.

To reset the IPMI

1. Log on to the Access Appliance shell menu.
2. Run the following command:

   ```
   Support > IPMI Reset
   ```

3. The following prompt displays:

   ```
    >> Resetting the IPMI disconnects all current IPMI users.
   Are you sure you want to reset the IPMI? [yes, no]:
   ```

   Type **yes** and press Enter.
4. The IPMI starts resetting in the background. Wait for 2 minutes before you attempt to reconnect to the Veritas Remote Management Console.
5. If you cannot access the Veritas Remote Management Console after resetting the IPMI, perform the following steps:
   - Schedule a convenient time for the appliance node shutdown and alert all users.
   - Shut down the appliance node.
   - Disconnect all power cables to the appliance node.
   - Wait for 15 seconds and then reconnect the cables.
   - Turn on the appliance node.

See “Configuring the IPMI port on an appliance node” on page 56.

See “Managing IPMI users on an appliance node” on page 56.

Setting the date and time on the appliance

You can set the date and time on the appliance as part of the initial configuration. After the cluster is configured, you should only change the time settings using the Veritas Access application interfaces.

See “How to configure the Access Appliance for the first time” on page 27.

You can manually set the time or configure the appliance to use a Network Time Protocol (NTP) server.

Note: Some appliance and Access functionality is dependent on keeping accurate time with the rest of your network environment. Veritas recommends that you use an NTP server for the appliance, as well as any hosts that it interacts with.

To set the date and time

1 Log on to the Access Appliance shell menu.

2 From the `Main_Menu > Network` view, type the following command to set the date and time:

```
Date Set <Month> <Day> <HH:MM:SS> <Year>
```

Where <*Month*> is the first three letters of the month, <*Day*> is the day of the month (1-31), <*HH:MM:SS*> is the hour, minute, and second in a 24-hour format, and <*Year*> is the year in `YYYY` format. For example:

```
Date Set Jun 2 15:12:00 2016
```

3 Type the following command to set the time zone:

```
TimeZone Set
```

In the menus that follow, type the numbers that correspond to the continent (or ocean), country, and time zone region where the appliance is located. When you complete your selections, type **yes** to set the time zone.

4 (Optional) Type the following command to configure the appliance to use an NTP server:

```
NTPServer Add <Server>
```

Where <*Server*> is the host name or IP address of the NTP server.

Chapter 7

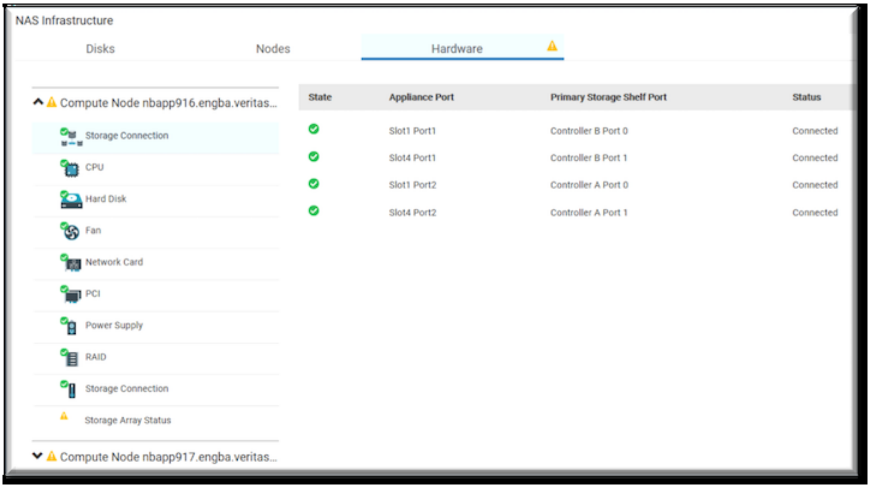
Monitoring the appliance

This chapter includes the following topics:

About hardware monitoring in the Access GUI

You can monitor the status of various appliance hardware components in the Veritas Access GUI. The hardware status is located under **NAS Infrastructure > Hardware**. You can view details about each node and the connected storage shelves.

Figure 7-1 Appliance hardware monitoring in the Veritas Access GUI



State	Appliance Port	Primary Storage Shelf Port	Status
✓	Slot1 Port1	Controller B Port 0	Connected
✓	Slot4 Port1	Controller B Port 1	Connected
✓	Slot1 Port2	Controller A Port 0	Connected
✓	Slot4 Port2	Controller A Port 1	Connected

See “Testing the appliance hardware” on page 66.

About Veritas AutoSupport on the Access Appliance

Veritas AutoSupport is a free service that enables proactive monitoring, management, and support of the appliance's health and performance 24 hours a day, 7 days a week. The AutoSupport service identifies risks and issues with the appliance and alerts you and/or service engineers to enable proactive handling and risk mitigation.

The Veritas AutoSupport service is delivered using two components: The appliance Call Home service and the MyAppliance web portal. When Call Home is enabled, the appliance uploads diagnostic and heartbeat data over SSL-encrypted channels to a Veritas secure operations center for further processing. The MyAppliance portal then uses the Call Home data to provide a comprehensive view of appliance health and performance information, as well as support case management.

AutoSupport technical details

- Call Home is enabled by default and uses HTTPS (secure and encrypted protocol) with port 443 for all communication with Veritas AutoSupport servers.
- If you configured the appliance to use a proxy server to connect to the Internet, Call Home uses that proxy server to communicate with the AutoSupport servers.
- The appliance initiates all communications with the AutoSupport servers.

For more information about the data that AutoSupport collects and when it is sent to Veritas, refer to the *Veritas Appliance AutoSupport 2.0 Reference Guide*.

See "Setting up AutoSupport on the appliance" on page 62.

Setting up AutoSupport on the appliance

Table 7-1 lists the steps that you need to carry out to set up AutoSupport for the appliance.

Table 7-1 Steps to set up AutoSupport

Step	Task
Step 1	Register the appliance on the MyAppliance portal. See "To register the appliance on the MyAppliance portal" on page 62.
Step 2	Enable Call Home on the appliance. **Note:** Call Home is enabled by default. See "To enable Call Home on the appliance" on page 62.

Step 1

To register the appliance on the MyAppliance portal

1. Log on to the Veritas MyAppliance portal.

   https://my.veritas.com/

2. On the **Appliances** page, click **My Appliances**.
3. Follow the prompts to register the appliance.

Step 2

To enable Call Home on the appliance

1. Log on to the Access Appliance shell menu.
2. From the `Main_Menu > Settings > Alerts` view, enter the following command:

   ```
   CallHome Enable
   ```

About moving an appliance to another geographic location

If you plan to move the appliance from one geographic location to another, consider the following points to ensure continuance of maintenance and support coverage:

- You should not move an appliance to another country.

- Certain locations or regions of the world may not be enabled or set up to handle field service calls for parts replacement.
- Certain locations or regions may not be able to meet the defined service level agreement (SLA) contract(s) to which the appliance may be associated with.
- If it is imperative to move the appliance, you must contact your account access team at Veritas to understand the ramifications or impact (if any) to the SLAs associated with the appliance.
- After you have moved the appliance, it is critical to update your registration details such as contact details and location information on the MyAppliance portal to ensure continuance of coverage.

Using a proxy server with the appliance

The following features require access to the Internet:

- AutoSupport (Call Home service)
- Automatic updates

Once you configure the appliance proxy settings, these services will travel through the proxy server.

To configure the appliance to use a proxy server

1. Log on to the Access Appliance shell menu on either node of the appliance.
2. From the `Main_Menu > Network > Proxy` view, type the following command:

   ```
   Set <Server:Port> [Tunnel] [Username]
   ```

   - *<Server>* - Type the IP address or host name of the proxy server, followed by a colon (:) and then the port number.
     If the proxy server requires https, add `https://` to the address. Otherwise the appliance adds `http://` to the address by default.
   - *[Tunnel]* - Type `TunnelOn` if your proxy requires tunneling (the default is `TunnelOff`).
   - *[Username]* - Type the appropriate user name if the proxy server requires authentication. You are prompted for a password after you execute the command.

   For example:

   ```
   Set https://proxy.example.company.com:80 TunnelOff ProxyAdmin123
   Enter password for user "admin":
   Successfully set proxy server
   ```

See "About Veritas AutoSupport on the Access Appliance" on page 61.

Setting up email notifications on the appliance

The appliance can send email alerts when hardware and software components fail or encounter errors.

To configure email notifications

1 Log on to the Access Appliance shell menu.

2 From the `Main_Menu > Settings > Alerts` view, enter the following command to set the SMTP mail server:

```
Email SMTP Add <server> [[account]] [[password]]
```

Where <*server*> is the IP address or FQDN of your SMTP mail server.

3 Enter one or both of the following commands to set the email addresses that you want the appliance to send emails to:

```
Email Hardware Add <hardware_admin>
```

```
Email Software Add <software_admin>
```

Where <*hardware_admin*> is the email address of the appliance hardware administrator and <*software_admin*> is the email address of the appliance software administrator.

Note: You can add multiple email addresses at once by separating them with a semi-colon (`;`). Do not add a space before or after the semi-colon.

4 Enter the following command to set the email account that you want the emails to originate from (sender email):*

```
Email SenderID Set <sender_email>
```

Where <*sender_email*> is the email address that you want the appliance emails to originate from.*

5 Enter the following command to set the time interval between email notifications:

```
Email NotificationInterval <minutes>
```

Where <*minutes*> is the time interval in minutes.

6 Enter the following command to verify the appliance email notification settings:*

```
Email Show
```

Note: Steps 4-6 are optional.

See "Setting up SNMP notifications on the appliance" on page 65.

Setting up SNMP notifications on the appliance

You can configure the appliance to generate and send Simple Network Management Protocol (SNMP) traps to your SNMP server for hardware monitoring purposes.

The appliance uses the SNMPv2-SMI application protocol.

To configure SNMP notifications

1 Log on to the Access Appliance shell menu.

2 From the `Main_Menu > Settings > Alerts` view, enter the following command to set the SNMP server:

```
SNMP Set <server> [[community]] [[port]]
```

Where <*server*> is the IP address or FQDN of your SNMP mail server.

Note: The appliance uses the default community `public` and the default destination port `162` for SNMP traps. If your SNMP server uses a different community or port, use the *[[community]]* and *[[port]]* variables.

Your firewall must allow access from the appliance to the SNMP server through whichever port you use.

3 Enter the following command to show the appliance MIB:

```
SNMP ShowMIB
```

Copy the Management Information Base (MIB) text and import it into your SNMP management software so that it can interpret the appliance traps.

4 Enter the following command to enable the SNMP configuration:

```
SNMP Enable
```

For information on how to send a test SNMP trap, refer to the following tech note:

www.veritas.com/docs/TECH208354

See "Setting up email notifications on the appliance" on page 64.

Testing the appliance hardware

Before making any significant hardware or software configuration changes (such as initial configuration and software upgrades), you should run a hardware self-test. This test helps ensure that there are no component cable errors or disk drive errors that can cause an operation to fail.

To test the appliance hardware

1. Log on to the Access Appliance shell menu of the appliance node.
2. From the `Main_Menu > Support` view, type the following command:

   ```
   Test Hardware
   ```

   A **Warning** indicates a problem that can be fixed later and lets you proceed with the initial configuration. However, such problems can prevent access to the affected devices.

   An **Error** indicates a critical problem that requires immediate resolution before you can proceed with the initial configuration.
3. (Optional) If the `Support > Test Hardware` command output identifies any problems, check the following items:

   - Verify that all cables are connected correctly and secured.
   - Verify that all disk drives are installed and seated properly.
   - Verify that all units are turned on and have started up completely.

   After you have verified the previous items, reenter the command to ensure that the problems are resolved. If you cannot resolve an error after verifying all of the previous items and reentering the command, contact Veritas Technical Support.

See “How to configure the Access Appliance for the first time” on page 27.

Resetting the appliance to factory settings

This chapter includes the following topics:

About appliance factory reset

The purpose of an appliance factory reset is to return your appliance node to a clean, unconfigured, and factory state. By default, a factory reset discards all storage configuration and data. However, before you initiate the factory reset, you can elect to retain the storage configuration, network configuration, and any existing data. In addition, you can elect to restart the appliance after the reset completes.

The Veritas Access Appliance supports two modes of factory reset:

- **Single node reset**
  Use this mode if you want to reset just one node and then add it back into the cluster. All of the data on the attached storage is preserved.
- **Full cluster reset**
  Use this mode if you want to reset the entire cluster and delete all data on the attached storage.

During the factory reset process, the following components are reset:

- Appliance operating system
- Appliance software

- Access software
- Storage configuration and data (optional)
- Networking configuration (optional)

See "Performing a single node factory reset" on page 68.

See "Performing a full appliance cluster factory reset" on page 70.

Performing a single node factory reset

To start a single node factory reset, you need to remove the appliance node from the cluster before you reset the node. Use the Access shell menu to remove the node, and then physically disconnect the Ethernet cables connecting the node to the cluster.

For more information about Veritas Access commands, refer to the *Veritas Access Appliance Command Reference Guide*.

Note: Do not reset the storage if you only want to reset a single node and preserve the cluster.

To perform a single node factory reset

1. Log on to the Access Appliance shell menu.
2. Enter the command `Main_Menu > Support > FactoryReset`.

   The screen layout shows, and it requires you to answer the following questions before the factory reset begins.

   ```
   >> Do you want to reset the network configuration as part of
   the factory reset? [yes, no](yes) no

   Select storage configuration and data reset [Optional]
           - Removes all data and backup images from the
             attached storage.
           - Resets the storage partitions.

   - [WARNING] Do not reset the storage unless you plan to
   factory reset the entire cluster. If you are resetting the
   entire cluster:
   Select ‘no’ when you are resetting the first node.
   Select ‘yes’ when you are resetting the last node.

   >> Do you want to reset the storage configuration and delete
   the data on the attached storage as part of the factory reset?
   (Select ‘no’ if you are resetting just a single node and want
   to preserve the cluster.) [yes, no](no) no

   >> A system restart is required to complete the factory reset.
   Do you want to automatically restart the node at the end of the
   factory reset process? [yes, no](no) yes
   ```

   Note: A known issue exists with selecting to not automatically restart the appliance. Veritas strongly recommends that you restart the appliance node at the end of the factory reset process. Refer to the *Veritas Access Release Notes* for more information about the known issue.

3. After you respond to these questions, the summary information displays.

4 The following warning appears. If you want to begin the factory reset operation, enter **yes**.

```
>> WARNING: The node is ready for factory reset. This process
cannot be reversed! Do you want to proceed? [yes, no] (no) yes
```

The factory reset continues and info messages are shown. It takes about 20 minutes to complete the factory reset process.

5 If you elected to reset the network configuration, you can no longer reach the Access Appliance shell menu over eth1. You must reconnect to the Access Appliance shell menu over IPMI.

Note: Once the factory reset is complete, you may need to install software release updates or EEB packages on the appliance node before you add the node back into the cluster. This is to ensure that the two nodes have the same software version, and install the same EEB packages. For more information about cluster commands, refer to the *Veritas Access Command Reference Guide*.

Performing a full appliance cluster factory reset

To reset the entire appliance cluster, you must perform the following tasks:

1. Remove the first node from the cluster.
2. Factory reset the first node, making sure not to reset the attached storage at this step.
3. Factory reset the second node and the attached storage.

For more information about Veritas Access commands, refer to the *Veritas Access Appliance Command Reference Guide*.

Note: A factory reset operation returns the password to the original, default value.

To perform a full appliance cluster factory reset

1 Remove the first node from the cluster.

2 Log on to the Access Appliance shell menu of the first appliance node.

3 Enter the command `Main_Menu > Support > FactoryReset`, and information messages show.

4. Select if you want to reset the network configuration and storage configuration. Make sure that you select `no`, when you see the following question:

   ```
   >> Do you want to reset the storage configuration and delete
   the data on the attached storage as part of the factory reset? (Select
   ‘no’ if you are resetting just a single node and want to preserve the
   cluster.) [yes, no](no) no
   ```

5. After you respond to these questions, the summary information displays.

6. The following warning appears. If you want to begin the factory reset operation, enter **yes**.

   ```
   >> WARNING: The node is ready for factory reset. This process cannot
   be reversed! Do you want to proceed? [yes, no] (no) yes
   ```

   Wait until the first node factory reset completes.

7. Log on to the Access Appliance shell menu of the second appliance node.

8. Enter the command `Main_Menu > Support > FactoryReset`, and information messages show.

   Make sure that you select `yes` to reset the storage:

   ```
   >> Do you want to reset the storage configuration and delete the
   data on the attached storage as part of the factory reset? (Select
   ‘no’ if you are resetting just a single node and want to preserve
   the cluster.) [yes, no](no)yes
   ```

9. The factory reset continues and the following message appears:

   ```
   -[Info] Running factory reset. This process can take up to 20 minutes...
   -[Info] The appliance is restarting...
   ```

See “About appliance factory reset” on page 67.

See “Performing a single node factory reset” on page 68.

Chapter 9

Appliance security

This chapter includes the following topics:

About Access Appliance security

Access Appliance Access appliances are developed from their inception with security as a primary need. Each element of the appliance, including its Linux operating system and the core Access application, is tested for vulnerabilities using both industry standards and advanced security products. These measures ensure that exposure to unauthorized access and resulting data loss or theft is minimized.

Each new version of Access appliance software and hardware is verified for vulnerabilities before release. Depending on the severity of issues found, Veritas releases a patch or provides a fix in a scheduled major release. To reduce the risk of unknown threats, Veritas regularly updates the third-party packages and modules in the product as part of regular maintenance release cycles.

About Access appliance user account privileges

Local user accounts are one mechanism to prevent unauthorized access to Access data on the appliance. Only the `admin` user can configure and modify appliance settings.

The following are some of the tasks that can be performed by appliance local users:

- Log on to the Access Appliance shell menu over ssh
- Monitor hardware and storage
- Audit SDCS logs
- Configure settings like date and time, networking, etc.
- Create checkpoints and rollback the appliance
- Apply patches and upgrade the appliance

Access appliance admin password specifications

Table 9-1 Password specifications

Description	Requirement
Maximum length	None
Minimum length	8 characters
Requirements	■ At least one lower case letter (a-z) ■ At least one number (0-9)
Restrictions	Passwords cannot: ■ Include non-alphanumeric characters, such as special characters (!, $, #, %, etc.) ■ Include spaces or / ■ Include dictionary words ■ Be the same or similar to the last seven passwords
Password expiration	Does not expire
Password lockout	None

Password encryption and handling on the Access appliance

The Access appliance uses the following password encryption measures:

- All local users (including `admin`, `maintenance`, and `root`) use SHA-512 password encryption.
- The past seven passwords are encrypted and logged for each user to enforce the password policy.
- User passwords are in transit in the following situations:
  - Logging on to the Access Appliance shell menu over SSH where the password is protected by the SSH protocol.

Changing the Maintenance user account password

Note: The Maintenance user password on each node must be the same or else the cluster configuration fails during the appliance initial configuration.

The appliance is preconfigured with a Maintenance user account. This account is used during the initial appliance configuration process to configure the various subsystems of the appliance and Veritas Access. The `Support > Maintenance` command also lets you log into this account and opens a separate shell that you can use to troubleshoot or manage underlying operating system tasks.

Warning: The Maintenance user account ships with a known default password. Veritas recommends that you change the default password before the Access cluster is configured.

After the cluster configuration is complete, you cannot change the Maintenance password.

The appliance does not support setting the Maintenance password by using commands such as `passwd maintenance`. You should use the Access Appliance shell menu to change the Maintenance account password.

To change the Maintenance user account password on an unconfigured appliance node

1. Log on to the Access Appliance shell menu of the appliance node.
2. From the `Main_Menu > Settings` view, type the following command:

   ```
   Password maintenance
   ```

3 Enter the existing Maintenance user password and then enter the new password.

The default password for the Maintenance user account is **P@ssw0rd** (where 0 is a zero).

4 Repeat this procedure for all other nodes to keep them in sync.

See "How to configure the Access Appliance for the first time" on page 27.

About the Access Appliance intrusion detection system

The Access appliance uses Symantec Data Center Security: Server Advanced (SDCS) software to monitor appliance software components for unauthorized access. SDCS is a security solution offered by Symantec to protect servers in data centers and is automatically configured during appliance software installation.

SDCS offers policy-based protection and helps secure the appliance using host-based intrusion detection technology. The SDCS agent launches automatically at startup and enforces the customized Access appliance intrusion detection system (IDS) policy. The IDS policy operates in real time for monitoring significant system events and critical configuration changes. This solution provides enhanced visibility into important user or system actions to ensure a valid and complete audit trail that addresses compliance regulations (such as PCI) as a compensating control.

The following list contains some of the events that the IDS policy monitors:

- User logons, logouts, and failed logon attempts
- `sudo` commands
- User addition, deletion, and password changes
- User group addition, deletion, and member modifications
- System auto-start option changes
- Modifications to all system directories and files, including core system files, core system configuration files, installation programs, and common daemon files
- Access services start and stop
- File and directory behavior to detect rootkits, worms, malicious modules, suspicious permission changes, etc.
- Audit of all the activity in the Access Appliance shell menu, including the shell operations by the `maintenance` and `root` users.

See "Reviewing SDCS events on the Access Appliance" on page 76.

See “Auditing the SDCS logs on an Access Appliance” on page 76.

Reviewing SDCS events on the Access Appliance

The SDCS logs can help in detecting security breaches and abnormal activity on the appliance.

The SDCS logs include some the following details for each event:

- When - The timestamp of the logged event.
- Who - Which user(s) was logged on when the event took place.
- What - The description of the event and the resource involved.
- How - The process name, process ID, operation permissions, and sandbox details.
- Severity - The severity of the event.

See “About the Access Appliance intrusion detection system” on page 75.

See “Auditing the SDCS logs on an Access Appliance” on page 76.

Auditing the SDCS logs on an Access Appliance

There are several ways to audit the SDCS logs on a Veritas Access Appliance node.

Basic search

To do a basic SDCS log search

1. Log on to the Access Appliance shell menu.
2. From the `Main_Menu > Monitor > SDCS` view, enter the following command:

   ```
   Audit Search <term>
   ```

   Where *<term>* is a word or name that you want to search in the logs for.

Filter by individual attribute

SDCS events have three main attributes:

- Date
- Severity
- Event type

You can filter the SDCS logs by each individual attribute.

To filter SDCS log entries by date

1. Log on to the Access Appliance shell menu.
2. Go to the `Main_Menu > Monitor > SDCS` view.
3. (Optional) Enter the following command to view all of the events that occurred on a specific day:

   ```
   Audit View Date <ToDate>
   ```

   Where <*ToDate*> is the day in the `DD/MM/YYYY` format.
4. (Optional) Enter the following command to view all of the events that occurred during a specific period of time:

   ```
   Audit View Date <ToDate>[-hh:mm:ss] [<FromDate>[-hh:mm:ss]]
   ```

   Where *<ToDate>[-hh:mm:ss]* is the later date/time and *[<FromDate>[-hh:mm:ss]]* is the earlier date/time. For example:

   ```
   Audit View Date 05/25/2016-13:00:00 05/25/2016-12:00:00
   ```

To filter SDCS log events by severity

1. Log on to the Access Appliance shell menu.
2. From the `Main_Menu > Monitor > SDCS` view, enter the following command:

   ```
   Audit View Severity <SeverityCode>
   ```

   Where <*SeverityCode*> is the one letter code of the severity type that you want to filter by.

   See "About SDCS event type codes and severity codes on an Access appliance node" on page 79.

To filter SDCS log entries by type

1. Log on to the Access Appliance shell menu.
2. From the `Main_Menu > Monitor > SDCS` view, enter the following command:

   ```
   Audit View EventType <TypeCode>
   ```

   Where <*TypeCode*> is the four letter code of the event type that you want to filter by.

   See "About SDCS event type codes and severity codes on an Access appliance node" on page 79.

Filter using multiple attributes

The best way to search for a specific type of SDCS event from a particular period of time is to use the `Audit View Filter` command.

To filter SDCS log entries by date

1. Log on to the Access Appliance shell menu.
2. From the `Main_Menu > Monitor > SDCS` view, enter the following command:

```
Audit View Filter <SeverityCode> <TypeCode> <ToDate>[-hh:mm:ss]
[<FromDate>[-hh:mm:ss]] <Search_yes/no>
```

- *<SeverityCode>*
  The one letter code of the severity type that you want to filter by. Enter **ALL** if you want to include all severity codes in your filter.
- *<TypeCode>*
  The four letter code of the event type that you want to filter by. Enter **ALL** if you want to include all event type codes in your filter.
- *<ToDate>[-hh:mm:ss] [<FromDate>[-hh:mm:ss]]*
  Where *<ToDate>[-hh:mm:ss]* is the later date/time and *[<FromDate>[-hh:mm:ss]]* is the earlier date/time. Use the `DD/MM/YYYY` date format.
  To filter events for a specific day, use *<ToDate>[-hh:mm:ss]* and type **NULL** for *[<FromDate>[-hh:mm:ss]]*.
  To filter all events after a specific date/time, use *[<FromDate>[-hh:mm:ss]]* and type **NULL** for *<ToDate>[-hh:mm:ss]*
- *<Search_yes/no>*
  Enter **yes** if you want to include a search term. Otherwise, enter **no**.

For example:

```
Audit View Filter C ALL 05/26/2016-14:00:00 05/25/2016-13:00:00
no
```

3. (Optional) If you entered **yes** for *<Search_yes/no>*, enter the search string when prompted.

Get more details about an event

You can use the `Audit View EventID` command to get more information about a specific SDCS event that is listed in a search or filter.

To get more details about a specific SDCS event

1. Log on to the Access Appliance shell menu.
2. From the `Main_Menu > Monitor > SDCS` view, enter the following command:

```
Audit View EventID <ID#>
```

Where *<ID#>* is the ID number of an event that was listed in your filter or search.

See "About the Access Appliance intrusion detection system" on page 75.

See "Reviewing SDCS events on the Access Appliance" on page 76.

About SDCS event type codes and severity codes on an Access appliance node

Table 9-2 SDCS severity codes

Code	Description	Details
C	Critical	Activity or problems that might require administrator intervention to correct.
E	Error	
I	Information	Information about normal system operation.
M	Major	A more serious event than Warning, but less serious than Critical.
N	Notice	Information about normal system operation.
T	Tracking	
W	Warning	Unexpected activity or problems that have already been handled by SDCS. **Note:** These messages might indicate that a service or application on the appliance is not functioning properly with the applied policy.

Note: You can also get this list of SDCS severity codes by typing the following command in the Access Appliance shell menu:

```
Main_Menu > Monitor > SDCS > Audit View SeverityCodes
```

Table 9-3 SDCS event codes

Code	Description
DAUD	IDS Audit
DFWU	File Watch Unix
DFWW	File Watch Windows
DGEN	Generic Log

Table 9-3 SDCS event codes *(continued)*

Code	Description
DIPS	IPS to IDS Event
DNTL	NT Event Log
DRGW	Registry Watch
DSYS	SysLog
DUC2	Unix C2 Security
DWTM	WTMP/BTMP
MBIN	Server Error
MCOM	Common Status
MCON	Agent Config Status
MEFR	File Received
MERR	IDS Error
MOVR	Agent Override
MREP	File Create
MSTA	Agent Status
MSTD	IDS Status
MSTP	IPS Status
PBOP	IPS Overflow
PCRE	IPS Create
PDES	IPS Destroy
PFIL	IPS File
PMNT	IPS Mount
PNET	IPS Network
POSC	IPS System Call
PPST	IPS PSET

Table 9-3 SDCS event codes *(continued)*

Code	Description
PREG	IPS Registry
TRAC	Tracking/Debugging

Note: You can also get this list of SDCS event type codes by typing the following command in the Access Appliance shell menu from the `Main_Menu > Monitor > SDCS` view:

```
Audit View EventTypeCodes
```

See “Auditing the SDCS logs on an Access Appliance” on page 76.

Changing the SDCS log retention settings on an Access appliance node

By default, the Veritas Access 3340 Appliance Appliance stores each SDCS log entry for 30 days. You can adjust this retention period to any number of days. However, if disk space becomes a factor, you can choose to retain a set amount of log files (each log file is ~10.5 MB).

You can check the current SDCS log retention settings for the appliance at any time using the `Audit ShowSettings` command in the `Main_Menu > Monitor > SDCS` view.

To change the SDCS log retention settings

1 Log on to the Access Appliance shell menu.

2 From the `Main_Menu > Monitor > SDCS` view, enter one of the following commands:

- To set the number of days in the retention period:

  ```
  Audit SetSettings RetentionPeriod <days>
  ```

  Where *<days>* is the specific number of days that you want the appliance to retain each log entry.

- To set the number of log files the appliance retains:

  ```
  Audit SetSettings FileNumber <files>
  ```

  Where *<files>* is the specific number of SDCS log file that you want the appliance to retain at any given time.

About Access appliance operating system security

The Access appliance runs a customized Linux operating system (OS) provided by Veritas. Each new appliance software release includes the latest appliance OS, Access software, bug fixes, and security patches. In addition to regular security patches and updates,

The appliance OS and software platform include the following security enhancements and features:

- An updated and trimmed Red Hat Enterprise Linux (RHEL)-based OS platform that enables the packaging and installation of all the necessary software components on a compatible and a robust hardware platform.
- Symantec Data Center Security: Server Advanced (SDCS) intrusion detection software.
- Regular scans of the appliance with industry-recognized vulnerability scanners.

  Any discovered vulnerabilities are patched in regular releases of the appliance software and (if necessary) with emergency engineering binaries (EEBs). If security threats are identified between release schedules, you can contact Veritas Technical Support for a known resolution.
- Nonusers and unused service accounts are removed or disabled.
- The appliance OS includes edited kernel parameters that secure the appliance against attacks such as denial of service (DoS).

  For example, the `sysctl` setting `net.ipv4.tcp_syncookies` is added to the `/etc/sysctl.conf` configuration file to implement TCP SYN cookies.
- Unnecessary runlevel services are disabled.

  The appliance OS uses runlevels to determine the services that should be running and to allow specific work to be done on the system.
- `FTP`, `telnet`, and `rlogin (rsh)` are disabled.

  Usage is limited to `ssh`, `scp`, and `sftp`.
- TCP forwarding for SSH is disabled with the addition of `AllowTcpForwarding no` and `X11Forwarding no` to `/etc/ssh/sshd_config`.
- IP forwarding is disabled on the appliance OS and does not allow routing on the TCP/IP stack.

  This feature prevents a host on one subnet from using the appliance as a router to access a host on another subnet.
- The Veritas Access 3340 Appliance Appliance does not allow IP aliasing (configuring multiple IP addresses) on the network interface.

This feature prevents access to multiple network segments on one NIC port.

- The UMASK value determines the file permission for newly created files.

  UMASK specifies the permissions which should not be given by default to the newly created file. Although the default value of UMASK in most UNIX systems is 022, UMASK is set to 077 on the appliance.
- The permissions of all the world-writable files that are found in the appliance OS are searched and fixed.
- The permissions of all the orphaned and unowned files and directories that are found in the appliance OS are searched and fixed.

Vulnerability scanning of the Access Appliance

Veritas regularly tests the Veritas Access Appliance with industry-recognized vulnerability scanners. Any new vulnerabilities that pose a security threat to the appliance are then patched in routine software releases. For high-severity vulnerabilities, Veritas may choose to issue a patch in an emergency engineering binary (EEB).

Table 9-4 lists the software products that were used to scan the Access appliance.

Table 9-4 Security scanners used for testing Veritas Access appliances

Security scanner	Version
Nessus™	6.8.1
QualysGuard™	8.9.2.1-1

Disabled service accounts on the Access appliance

The following service accounts are disabled in the appliance operating system and software platform:

- Batch jobs daemon
- bin
- DHCP server daemon
- FTP account
- User for haldaemon
- User for OpenLDAP
- Mailer daemon
- Manual pages viewer

- User for D-BUS
- Name server daemon
- News system
- nobody user
- NTP daemon
- PolicyKit
- Postfix Daemon
- SSH daemon
- Novell Customer Center User
- UNIX-to-UNIX CoPy system
- wwwrun WWW daemon Apache
- NBE Web service ntbecmlpi

About data security on the Access appliance

The Access appliance uses policy-driven mechanisms to protect data in your Access environment.

Data security is improved by using the following measures to avoid data leaks:

- Real-time intrusion detection mechanisms to audit access to confidential data
- Logging and real-time tracking of all restores.
- Access to the backed up data is only granted to authenticated appliance users and processes.
- All backed up data in storage (VPFS) is marked with Cyclic Redundancy Check (CRC) digital signatures when the backup takes place. A maintenance task continuously re-computes the CRC digital signatures and compares it with the original signature to detect if there has been any unwanted tampering or corruption in the storage.
- Encryption of data in transit and at rest for services like the Veritas Cloud Service and AutoSupport.

About data integrity on the Access appliance

The VPFS storage on the appliance provides the following data integrity checks to ensure successful access to copy data:

- Continuous end-to-end verification of copy data in the Access storage pool

  Any inadvertent data modifications that can cause data corruption are automatically detected and rectified if possible.

- Continuous cyclic redundancy check (CRC) verification of copy data in the Access storage pool

  A CRC value is computed for each object created for copy data in Access storage. A background process continuously verifies the CRC signatures to ensure that backup data is not tampered with and can be restored successfully when needed. The Access storage design naturally isolates any data corruption from uncorrupted portions of the storage pool, preventing corruption from spreading throughout the entire pool.

Recommended IPMI settings on the Access appliance

Review this section to ensure that the Veritas Remote Management Console and the IPMI port are secure.

Users

- Do not allow accounts with null user name or password.
- It is recommended to have one administrative user.
- It is recommended to disable the anonymous user.
- To mitigate the CVE-2013-4786 vulnerability:
  - Use strong passwords to limit the effectiveness of offline dictionary attacks and brute force attacks. The recommended password length is 16-20 characters.
  - Change the password of the default user (`sysadmin`) as soon as possible.
  - Use Access Control Lists (ACLs) or isolated networks to limit access to the IPMI interface.

Login

Table 9-5 Login security settings

Settings	Recommended values
Failed login attempts	3
User Lockout time (min)	60 seconds

Table 9-5 Login security settings *(continued)*

Settings	Recommended values
Force HTTPS	Yes The **Force HTTPS** check-box must be enabled to ensure that the IPMI connection always takes place over HTTPS.
Web Session Timeout	1800

LDAP Settings

Veritas recommends that you should enable LDAP authentication, if possible in your environment.

SSL Upload

Veritas recommends that you import a new or custom SSL certificate.

Remote Session

Table 9-6 Remote session security settings

Settings	Recommended values
KVM Encryption	AES
Media Encryption	Enable

Cipher recommendation

- Do not set cipher to zero on the IPMI channel

  Warning: If the cipher 0 enabled on a channel, it allows anyone to perform any IPMI action with no authentication, effectively subverting IPMI security entirely. Disable it at all costs.

- Only use ciphers 3, 8, and 12.

Ethernet connection settings

Recommended to have a dedicated Ethernet connection for IPMI, that is you should avoid sharing the server's physical connection.

- Use a static IP
- Avoid DHCP

Replacing the default IPMI SSL certificate on the Access appliance

Use the following procedure to create a minimal self-signed certificate on a Linux computer and import it into the IPMI web interface:

To create and implement a minimal self-signed certificate

1. On a Linux computer, type the following command to generate the private key:

   ```
   openssl genrsa -out ipmi.key 2048
   ```

   In this case, the private key is named `ipmi.key`.

2. Type the following command to generate a certificate signing request (`ipmi.csr`) using `ipmi.key`:

   ```
   openssl req -new -key ipmi.key -out ipmi.csr
   ```

   Fill in each field with the appropriate values. To leave a field blank, enter a period (**.**).

   Note: To avoid extra warnings in your browser, set the common name to the fully qualified domain name of the IPMI interface.

3. Type the following command to sign `ipmi.csr` with `ipmi.key` and create a certificate called `ipmi.crt` that is valid for 1 year:

   ```
   openssl x509 -req -in ipmi.csr -out ipmi.crt -signkey ipmi.key
   -days 365
   ```

4. Type the following command to concatenate `ipmi.crt` and `ipmi.key` to create a certificate in PEM format called `ipmi.pem`:

   ```
   cat ipmi.crt ipmi.key > ipmi.pem
   ```

5. Log on to the Veritas Remote Management Console.

   Note: If you need to access the Veritas Remote Management Console from another computer, copy the `ipmi.pem` file to that computer.

6 On the **Configuration** tab, select **SSL** from the left pane.

Next to **New SSL Certificate**, click **Browse...** and select the `ipmi.pem` file.

Click **Upload**.

Note: A warning may appear that says an SSL certificate already exists. Press **OK** to continue.

---

7 Click **Browse...** again to import the privacy key. (Note that it now says **New Privacy Key** next to the button instead of **New SSL Certificate**.)

Select the `ipmi.pem` file and click **Upload**.

When the confirmation dialog appears, click **OK** to restart the web service.

8 (Optional) Close and reopen the Veritas Remote Management Console to verify that the new certificate is being presented.

Chapter 10

Troubleshooting

This chapter includes the following topics:

- About appliance log files
- Viewing log files using the Support command
- Gathering device logs with the DataCollect command

About appliance log files

Log files help you to identify and resolve any issues that you may encounter with the appliance.

The Veritas Access Appliance captures software-, system-, and performance-related data in log files. This data offers information about things like appliance operation, issues, and processes.

Appliance logs also help with the diagnosis of hardware-related issues, such as unconfigured volumes or arrays, temperature irregularities, and battery malfunction.

Table 10-1 describes the methods you can use to access the appliance log files.

Table 10-1 Methods of accessing appliance logs

Method	Log details
Download logs to a remote computer. Log onto the Access Appliance shell menu and download the appliance unified logs or appliance device logs.	■ Appliance unified logs ■ Appliance storage device logs
View You can use the `Main > Support > Logs > VxLogView` commands to access the appliance VxUL (unified) logs.	Appliance unified logs

Table 10-1 Methods of accessing appliance logs *(continued)*

Method	Log details

You can use the `Main > Support > Logs > Browse` command to access the appliances logs in the following directories:
- <DIR> ACCESS
- <DIR> APPLIANCE
- <DIR> OS
- <DIR> COREDUMP
See "Viewing log files using the Support command" on page 90.
	- Selftest report
	`LOGROOT/APPLIANCE/selftest_report`
	- Host change log
	`LOGROOT/APPLIANCE/log/hostchange.log`
	- Operating system (OS) installation log
	  - `LOGROOT/APPLIANCE/OS/var/log/boot.log`
	  - `LOGROOT/APPLIANCE/OS/var/log/messages`

You can use the `Main > Support > DataCollect` commands to collect storage device logs. See "Gathering device logs with the DataCollect command" on page 91.	Appliance storage device logs

Viewing log files using the Support command

You can use the following section to view the log file information.

To view logs using the `Support > Logs > Browse` command:

1. Log onto the Access Appliance shell menu of the desired node.
2. From the `Main_Menu > Support > Logs` view, type the following command:

   ```
   Browse
   ```

   The `LOGROOT/>` prompt appears.
3. To display the available log directories on the appliance, type `ls` at the `LOGROOT/>` prompt.
4. To see the available log files in any of the log directories, use the `cd` command to change directories to the log directory of your choice. The prompt changes to show the directory that you are in. For example, if you changed directories to the `APPLIANCE` directory, the prompt appear as `LOGROOT/APPLIANCE/>`. From that prompt you can use the `ls` command to display the available log files in the `APPLIANCE` log directory.
5. To view the files, use the `less <FILE>` or `tail <FILE>` command. Files are marked with `<FILE>` and directories with `<DIR>`.

To view Access Appliance unified (VxUL) logs using the `Support > Logs` **command:**

1. Log onto the Access Appliance shell menu of the desired node.
2. Enter the `Support > Logs` view.
3. Type the following the command:

   ```
   VXLogView Module
   ```

   The command shows a list of log directories. Type the number that corresponds to the appliance system component that contains the module that you want to view the VxLog of.

Note: Log recycling has been enabled, and the default number of log files has been set to 50.

See "Gathering device logs with the DataCollect command" on page 91.

See "About appliance log files" on page 89.

Gathering device logs with the DataCollect command

You can use the `DataCollect` command from the `Main_Menu > Support` view to gather device logs. You can share these device logs with the Veritas Support team to resolve device-related issues.

Along with the operating system, IPMI, and storage logs, the DataCollect command now collects the following logs as well:

- Access product logs
- Command output logs
- Patch logs
- File System logs
- Test hardware logs
- CPU information
- Disk performance logs
- Memory information
- Hardware information

To gather device logs with the DataCollect command

1. Log on to the Access Appliance shell menu of the desired node.
2. Enter the `Main_Menu > Support` view.

3 Type the `DataCollect` command to gather storage device logs.

```
Gathering release information
Gathering disk performance logs
Gathering command output logs
Gathering dmidecode logs
Gathering ipmitool sel list logs
Gathering ipmitool sel writeraw logs
Gathering fwtermlog logs
Gathering AdpEventLog logs
Gathering smartctl logs
Gathering ipmiutil command output
Gathering BMC Debug logs
Gathering Seagate storage array logs
Gathering cpu information
Gathering memory information
Gathering os logs
Gathering dfinfo logs
Gathering vxprint logs
Gathering patch logs
Gathering autosupport logs
Gathering sysinfo logs
Gathering sdr logs
Gathering adpallinfo logs
Gathering encinfo logs
Gathering cfgdsply logs
Gathering cfgdsply logs for LTR
Gathering ldpdinfo logs
Gathering pdlist logs
Gathering fru logs
Gathering adpbbucmd logs
Gathering sas3ircu logs
Gathering sas3ircu display logs
Gathering adpalilog logs
Gathering Test Hardware logs
Gathering Access product logs


All logs have been collected in /tmp/DataCollect.zip
Log file can be collected from the appliance shared folder - \\\logs\APPL
Share can be opened using Main->Support->Logs->Share Open
The Log files DataCollect-XXXX9000918-20180201012500.tar.gz collected fro
appliance are sent to AutoSupport servers.
```

```
The data transmission may complete in several minutes or longer due to fi
, network status, appliance performance and other reasons.
=======================End of DataCollect================================
```

The appliance generates the device log in the `/tmp/DataCollect.zip` file.

4. Copy the`/tmp/DataCollect.zip` to your local folders by using the `Main > Support > Logs > Share Open` command.

5. You can send the `DataCollect.zip` file to the Veritas Support team to resolve your issues.

See “About appliance log files” on page 89.