Veritas Access Appliance Initial Configuration Guide

VERITAS™

Access Appliance Initial Configuration Guide

Last updated: 2023-06-19

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

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

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

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.

See “About the Access Appliance administration interfaces” on page 6.

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 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 ■ Hardware maintenance ■ Appliance upgrade ■ Appliance troubleshooting
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.

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

Interface	Description
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: https://*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 8.

See "About the Veritas Remote Management Console" on page 43.

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 in to the Access Appliance shell menu, the following commands are availbale:

- configure Perform initial Access appliance tasks
- delete Delete appliance settings
- export Export appliance settings
- import Import appliance settings
- set Modify appliance settings
- show Examine the running and historical state of the host
- start Run appliance commands
- support Perform supportability operations
- system Run a privileged operation or obtain monitoring data

Helpful tips

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

- For a list of available commands, type question mark (**?**).
- For a list of shell shortcuts, press **Alt+s**.
- To get more information about a command, type '**?**' while typing or after using a tab to auto-complete the command.

See "About the Access Appliance administration interfaces" on page 6.

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 enforcement of Veritas Access licensing

Enforcement	Action
During Validity	None
During Grace period	Persistent message (in the GUI only)
Post Grace Period	Persistent message (in the GUI only)

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

- 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:

- 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 that is installed on each node of the cluster.

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 3350 Appliance Product Description*
- *Veritas Access 3350 Appliance Hardware Installation Guide*
- Veritas Access Appliance Cloud Storage Tiering Solutions Guide
- Veritas Access Appliance Solutions Guide for Enterprise Vault
- Veritas Access Appliance Solutions Guide for NetBackup
- Veritas Access Appliance Troubleshooting Guide
- Veritas Access Appliance Administrator's Guide
- Veritas Access Appliance Release Notes
- *Veritas Appliance AutoSupport 2.0 Reference Guide*
- *Veritas Access Appliance Safety and Maintenance Guide*
- *Veritas Access Appliance Third-Party Legal Notices Guide*
- *Veritas Access Appliance Upgrade Guide*

Chapter 2

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.

Network information

For the appliance itself, you 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 AutoSupport services)
- Static route and other advanced routing information
- IP address or the FQDN of the Network Time Protocol (NTP) server. If you use an FQDN for the NTP server, you must configure the DNS 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. The IP address assigned to the eth1 network interface must be resolved to a valid host name via the DNS server lookup or the local hosts file. A unique DNS entry is required for eth1 on each node.

The DNS server must be configured if you use the CallHome feature. Without the DNS entries, the AutoSupport client cannot send out alert emails and the system health collector cannot work properly.

You must also configure the DNS server if you use an FQDN for the NTP server.

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 is required when you perform operations that require access to the operating system.

You are required to change the factory default admin and maintenance passwords during the initial configuration.

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

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

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 45.
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 41.
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 16.

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.

You can configure a pure IPv4 or an IPv6 network, or a mixed mode network with both IPv4 and IPv6 addresses.

Note: The IP type (IPv4 or IPv6) can be different on different networks. In a single network, the IP type must be consistent (either IPv4 or IPv6).

Table 2-2

eth1	eth2 and eth3	eth4 and eth5 (for Access 3340 Appliance model) eth4 and eth6 (for Access 3350 Appliance model)	Console IP
IPv4	IPv4	IPv4	IPv4
IPv4	IPv4	IPv6	IPv4
IPv6	IPv4	IPv6	IPv6
IPv6	IPv4	IPv4	IPv6

You need to obtain a range of physical IP addresses, a 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. The range of IP addresses need not be contiguous as long as the IP addresses are in the same data network. 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
- Netmask for the data network
- Details for the private network, such as starting IP address and the netmask for the private IP address

- (Optional) IP address for the Domain Name System (DNS) server
- DNS domain name
- NTP server

Note: If the FQDN of the NTP server is specified, you are required to configure the DNS server.

IP address requirements

Table 2-3 Required IP addresses

Number of IPs	Item
0 to 4	Physical IP addresses for public network access over eth4 and eth5 for the Access 3340 Appliance model or over eth4 and eth6 for the Access 3350 Appliance model. You can configure up to four public IP addresses. The IP addresses are assigned to the public interfaces of both the nodes using the round-robin algorithm, selecting the first public interface of both the nodes followed by the second public interface of both the nodes.
0 to 8 (Optional)	Virtual IP addresses for public network access over eth4 and eth5 for the Access 3340 Appliance model or over eth4 and eth6 for the Access 3350 Appliance model. Starting with version 8.0, you can assign a virtual IP address to a public data network interface that does not have a physical IP address assigned to it. Earlier, a physical IP address was required to be assigned to a public data network interface if you wanted to assign a virtual IP address to it.
1	IP address for the management console.
2	IP addresses for or appliance node management over IPMI. See "Initial configuration requirements" on page 11.
2	IP addresses for appliance node management over eth1. See "Initial configuration requirements" on page 11.

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

See "Where to find the documentation" on page 10.

See “Network and firewall requirements” on page 16.

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.

For the Access 3340 Appliance model, 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. For the Access 3350 Appliance model, when you configure network bonding for public network access, bond0 is created, which groups eth4 (pubeth0) and eth6 (pubeth2) 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 maximum of two public IP addresses for public network access. The IP addresses need not be contiguous.
- Reserve one virtual IP address for the Remote Management Console.

Network and firewall requirements

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 2-4 lists the ports open for inbound communication to the appliance.

Table 2-4 Inbound ports

Port	Service	Description	Open on interface (3340 model)	Open on interface (3350 model)
22	ssh	In-band management CLI	eth1, eth2, eth3, eth4, eth5	eth1, eth4, eth5, eth6, eth7

Table 2-4 Inbound ports *(continued)*

Port	Service	Description	Open on interface (3340 model)	Open on interface (3350 model)
443	HTTPS	In-band management GUI	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
623	KVM	(optional, used if open)	eth4, eth5	eth4, eth5, eth6, eth7
2049	HTTPS	NFS++	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
445	CIFS SAMBA	CIFS (for the Log/Install shares)	eth1, eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7
10082	spoold	Veritas Data Deduplication engine	eth4, eth5	eth4, eth5, eth6, eth7
10102	spad	Veritas Data Deduplication manager	eth4, eth5	eth4, eth5, eth6, eth7

* Veritas Remote Management – Remote Console

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

Table 2-5 lists the ports outbound from the appliance to allow alerts and notifications to the indicated servers.

Table 2-5 Outbound ports

Port	Service	Description	Open on interface (3340 model)	Open on interface (3350 model)
443	HTTPS	Call Home notifications to Veritas Download SDCS certificate	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7

Table 2-5 Outbound ports *(continued)*

Port	Service	Description	Open on interface (3340 model)	Open on interface (3350 model)
162**	SNMP	Traps sent by SNMP agents	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
22	SFTP	Log uploads to Veritas	eth1, eth2, eth3, eth4, eth5	eth1,eth4,eth5, eth6, eth7
25	SMTP	Email alerts	eth1, eth4, eth5	eth1, eth4, eth5, eth6, eth7
389	LDAP	LDAP	eth1	eth1
636	LDAPS	Secure LDAP	eth1	eth1
514	rsyslog	Log forwarding	eth1, eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7
8514	Log transfer service	Log Transfer Console for downloading logs	eth1	eth1
10082	spoold	Veritas Data Deduplication engine	eth4, eth5	eth4, eth5, eth6, eth7
10102	spad	Veritas Data Deduplication manager	eth4, eth5	eth4, eth5, eth6, eth7

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

Table 2-6 lists the out of band management ports on the appliance.

Table 2-6 Out of band management ports

Port	Service	Description	Open on interface (3340 model)	Open on interface (3350 model)
80	HTTP	Out-of-band management (ISM+ or RM*)	eth4, eth5	eth4, eth5, eth6, eth7
443	HTTP	Out-of-band management (ISM+ or RM*)	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
623	KVM	(optional, used if open)	eth4, eth5	eth4, eth5, eth6, eth7
7578	RMM	CLI access	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
7582	RMM	KVM	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
2049	HTTPS	NFS ++	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
445		CIFS (for the Log/Install shares)	eth1, eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7

+ 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 2-7 displays the default ports that Access uses to transfer information.

Table 2-7 Default Veritas Access ports

Port	Protocol or Service	Purpose	Impact if blocked	Open on interface (3340 model)	Open on interface (3350 model)
22	SSH	Secure access to the Access server	Access is not accessible.	eth1, eth2, eth3, eth4, eth5	eth1, eth4, eth5, eth6, eth7
25	SMTP	Sending SMTP messages.	The SMTP messages that are sent from Access are blocked.	eth1, eth4, eth5	eth1, eth4, eth5, eth6, eth7
53	DNS queries	Communication with the DNS server	Domain name mapping fails.	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
111	rpcbind	RPC portmapper services	RPC services fail.	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
123	NTP	Communication with the NTP server	Server clocks are not synchronized across the cluster. NTP-reliant features (such as DAR) are not available.	eth1, eth4, eth5	eth1, eth4, eth5, eth6, eth7
139	CIFS	CIFS client to server communication	CIFS clients cannot access the Access cluster	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
161	SNMP	Sending SNMP alerts	SNMP alerts cannot be broadcast.	eth1, eth4, eth5	eth1, eth4, eth5, eth6, eth7

Table 2-7 Default Veritas Access ports *(continued)*

Port	Protocol or Service	Purpose	Impact if blocked	Open on interface (3340 model)	Open on interface (3350 model)
445	CIFS	CIFS client to server communication	CIFS clients cannot access the Access cluster.	eth1, eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7
514	syslog	Logging program messages	Syslog messages are not recorded.	eth1, eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7
756, 757, 755	statd	NFS statd port	NFS v3 protocol cannot function correctly.	eth1, eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7
2049	NFS	NFS client to server communication	NFS clients cannot access the Access cluster.	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
3172, 3173	ServerView	ServerView port	ServerView cannot work.	eth1, eth4, eth5	eth1, eth4, eth5, eth6, eth7
3260	iSCSI	SCSI target and initiator communication	Initiator cannot communicate with the target.	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
4001	mountd	NFS mount protocol	NFS clients cannot mount file systems in the Access cluster.	eth1, eth4, eth5	eth1,eth4,eth5, eth6, eth7

Table 2-7 Default Veritas Access ports *(continued)*

Port	Protocol or Service	Purpose	Impact if blocked	Open on interface (3340 model)	Open on interface (3350 model)
4045	lockd	Processes the lock requests	File locking services are not available.	eth1, eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7
5634	HTTPS	Management Server connectivity	Web GUI may not be accessible.	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
56987	Replication	File synchronization, Access replication	Access replication daemon is blocked. Replication cannot work.	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
8088	REST server	REST client to server communication	REST client cannot access REST API of Access.	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
8143	S3	Data port for Veritas Access S3 server	User will not able to use Veritas Access object server.	eth1, eth4, eth5	eth1, eth4, eth5, eth6, eth7
8144	ObjectAccess service	Administration port for Veritas Access S3 server.	User cannot create access or secret keys for using Objectaccess service.	eth1, eth4, eth5	eth1,eth4,eth5, eth6, eth7

Table 2-7 Default Veritas Access ports *(continued)*

Port	Protocol or Service	Purpose	Impact if blocked	Open on interface (3340 model)	Open on interface (3350 model)
11211	Memcached port	CLISH framework	CLISH cannot function correctly, and cluster configuration may get corrupted.	eth2	eth2
14161	HTTPS	Access Veritas Access GUI	User is unable to access Veritas Access GUI	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
51001	UDP	LLT over RDMA	LLT is not working.	eth2	eth2
51002	UDP	LLT over RDMA	LLT is not working.	eth2	eth2

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 2-8 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 2-8 Default NetBackup TCP and UDP ports

Port Range	Protocol	Open on interface (3340 model)	Open on interface (3350 model)
1556	TCP, UDP	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
13701-13702, 13705-13706	TCP	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7

Table 2-8 Default NetBackup TCP and UDP ports *(continued)*

Port Range	Protocol	Open on interface (3340 model)	Open on interface (3350 model)
13711, 13713, 13715-13717, 13719	TCP	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
13720-13722	TCP, UDP	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
13723	TCP	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
13724	TCP, UDP	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
13782-13783	TCP, UDP	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
13785	TCP	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7

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 2-9 lists additional CIFS ports and protocols.

Table 2-9 Additional CIFS ports and protocols

Port	Protocol	Purpose	Open on interface (3340 model)	Open on interface (3350 model)
53	TCP, UDP	DNS	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
88	TCP, UDP	Kerberos	eth4, eth5	eth4, eth5, eth6, eth7

Table 2-9 Additional CIFS ports and protocols *(continued)*

Port	Protocol	Purpose	Open on interface (3340 model)	Open on interface (3350 model)
139	TCP	DFSN, NetBIOS Session Service, NetLog	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
445	TCP, UDP	SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc	eth1, eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7
464	TCP, UDP	Kerberos change or set a password	eth1, eth2, eth3, eth4, eth5	eth1, eth2, eth3, eth4, eth5, eth6, eth7
3268	TCP	LDAP GC	eth4, eth5	eth4, eth5, eth6, eth7
4379	TCP	CTDB in CIFS	eth1,eth2, eth4, eth5	eth1, eth2, eth4, eth5, eth6, eth7

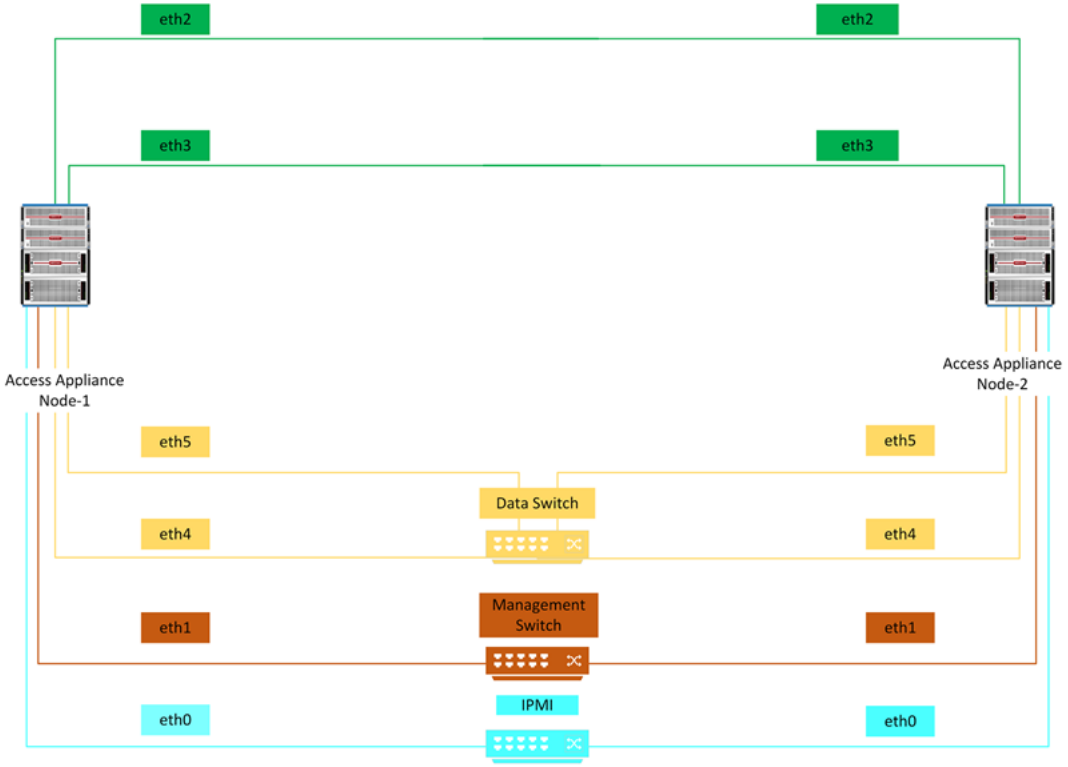
Table 2-10 lists the ports that are required for LDAP with SSL.

Table 2-10 LDAP with SSL ports

Port	Protocol	Purpose	Open on interface (3340 model)	Open on interface (3350 model)
636	TCP	LDAP SSL	eth1	eth1
3269	TCP	LDAP GC SSL	eth4, eth5	eth4, eth5, eth6, eth7

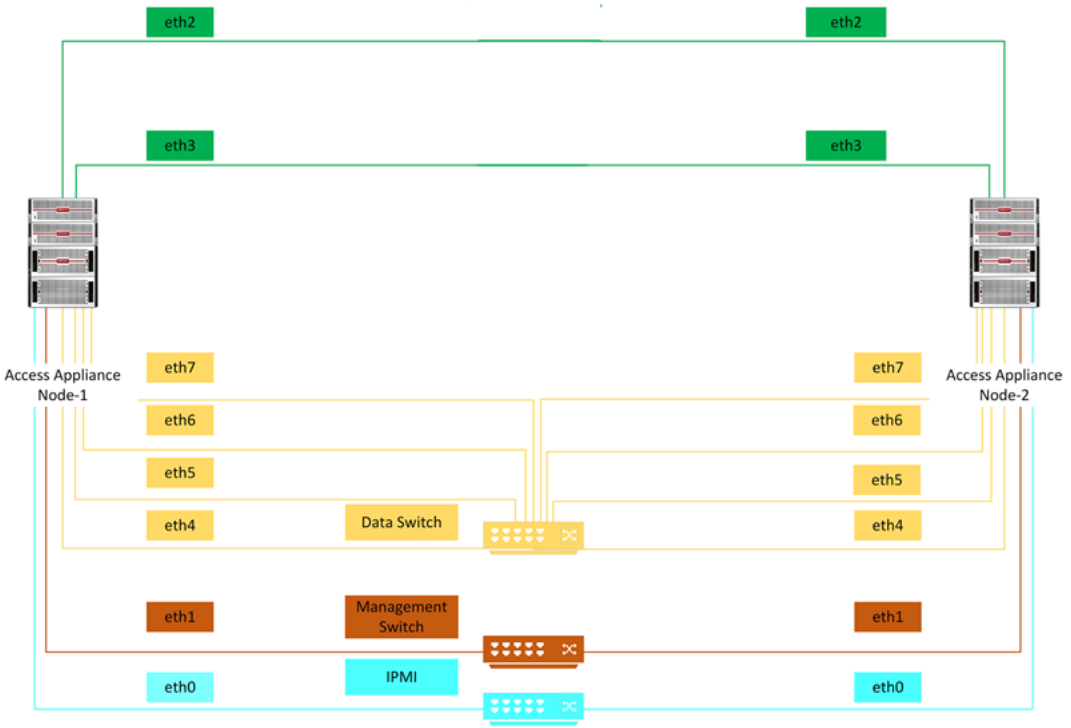
About network connections for the appliance

The following diagram shows how to connect the Access 3340 Appliance to the network. Note that the eth4 and eth5 public NICs must be plugged into the motherboard. Ensure that the appliance nodes are cabled as shown below:



Note: The management network and the data network can be the same.

The following diagram shows how to connect the Access 3350 appliance to the network. Note that the eth4 and eth6 public NICs must be plugged into the motherboard when you perform the initial cluster configuration. The eth5 and eth7 public NICs are optional and need not be plugged in. Ensure that the appliance nodes are cabled as shown below:



Note: The management network and the data network can be the same.

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

When you configure the Access cluster, you can configure a separate management network and a single separate data network if the management NIC and the public NICs are in different subnets. If you choose to configure a separate management and data network, ensure that you specify a console IP, which is in the management network IP range. After the initial cluster configuration is complete, you can configure additional data networks.

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 3350 Appliance Hardware Installation Guide*.
Step 2	Review the appliance initial configuration requirements. See "Initial configuration requirements" on page 11.

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 45.
Step 4	Run the hardware self-test on each node. See "Testing the appliance hardware" on page 53.

Step 5	Check the status of each node.
	`show appliance 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	Test the appliance software components. Run the `system self-test software` command. Ensure that the self test result displays **PASS**.
Step 7	Configure eth1 on both nodes. See "Configuring network address settings on the appliance nodes" on page 39.

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 8 (Recommended)	Configure the appliance to use a proxy server for AutoSupport and software updates. See "Setting up AutoSupport on the appliance" on page 49. See "Using a proxy server with the appliance" on page 50.
Step 9 (Recommended)	Configure the appliance to send notifications and alerts. See "Setting up email notifications on the appliance" on page 51. See "Setting up SNMP notifications on the appliance" on page 52.

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

Step	Task
Step 10	Perform the cluster configuration. See "Configuring the Access cluster on the appliance" on page 31. **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. For increased security, forced password changes are enforced during the initial cluster configuration to ensure known default passwords do not exist on the system. You must change the default passwords for the admin, maintenance, and IPMI user accounts. The GRUB and root passwords are set to the maintenance account password.
Step 11 (Optional)	Log in to the Access web interface (UI) as an `admin` user to configure storage. When you log in to the UI for the first time, you have the option to configure storage for long-term retention of data or skip directly to the **Dashboard**.

See "Where to find the documentation" on page 10.

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 28.

To configure the Veritas Access cluster on the appliance:

1. Log in to the Access Appliance shell menu of one of the appliance nodes using the default credentials:

   User: **admin**

   Password: **P@ssw0rd**

2. Enter the `configure cluster` command to start the cluster configuration wizard.

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 55 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.

Note: If you plan to use Active Directory authentication, Windows Active Directory restricts a NetBIOS name or a computer object name to a maximum of 15 characters. Access Appliance uses the first 15 characters of the cluster name to create a NetBIOS name to comply with the Windows AD restriction. Ensure that the chosen cluster name is unique in the first 15 characters so the objects created in the domain are distinct with unique names.

---

5 If VLAN is configured for the appliance, specify the VLAN ID for both the nodes.

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

7 Enter the maintenance user password for appliance nodes.

After specifying the password, the storage on each of the nodes is scanned. The data, fencing, and configuration volumes are created when you scan the storage. The configuration cannot proceed if the storage scan operation fails.

8 Specify whether you want to configure network bonding for the public network interfaces. For the Access 3340 Appliance model, you can configure network bonding for eth4 and eth5. For the Access 3350 Appliance model, you can configure network bonding for eth4 and eth6. To configure network bonding, type **yes** and continue to step 9; else type **no** and go to step 10.

9 If you typed **yes** in step 8, complete the following steps and go to step 13.

- 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 have 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 have reserved. At a minimum, you need to reserve two continuous virtual IP addresses.

See "About obtaining IP addresses for Veritas Access" on page 13.

10 Enter the number of public IP addresses that you want to configure for the public data network. You can specify any value from 0 to 4 considering each node of a 2-node Access cluster has two public network interfaces.

If you choose to configure one or more IP addresses, you are prompted to enter the specified number of IP addresses. You have the option to enter a maximum of 32 IP addresses. However, only the number of IP addresses that you specified are configured and the rest are maintained as free IP addresses in the cluster.

You can enter individual public IP addresses for the data network or an IP address range. You can specify IPv4 or IPv6 addresses. The addresses need not be contiguous. An IPv4 range is supported.

For example, to specify an IP range, type `10.182.12.89-92`.

The IP addresses are assigned to the public interfaces of both the nodes using the round-robin algorithm, selecting the first public interface of both the nodes followed by the second public interface of both the nodes. For example if you specify 3, the first public interface of both the nodes is assigned an IP address followed by the second public interface of the first node. If you specify 3 and choose to enter 4 IP addresses, the 3 IP addresses are assigned using the round-robin algorithm and 1 IP address is maintained as a free IP address in the cluster. If you enter 0, no public IP address is configured and you are not prompted to specify the IP addresses.

See "About obtaining IP addresses for Veritas Access" on page 13.

11 Enter the number of virtual IP addresses to assign to each network interface in the data network.

Note: Starting with version 8.0, you can assign a virtual IP address to a public data network interface that does not have a physical IP address assigned to it. Earlier, a physical IP address was required to be assigned to a public data network interface if you wanted to assign a virtual IP address to it.

---

12 Enter the starting virtual IP address or individual virtual IP addresses separated by a space or a comma. You can specify IPv4 or IPv6 addresses. The addresses need not be contiguous. An IPv4 range is supported.

13 Enter the netmask for the data network IP addresses.

14 Enter the gateway IP address of the data network.

15 Enter the console virtual IP address.

16 Enter the host name for the nodes.

The host name must be at least 3 and no more than 63 characters long.

17 Enter the IP address or the FQDN of the NTP server.

If you specify the FQDN of the NTP server, you must configure the DNS server. Enter the DNS server IP address and go to step 19. If you specify the IP address of the NTP server continue to step 18.

18 Specify whether you want to configure a DNS server.

If you opted to configure a DNS server, enter the DNS server IP address.

Note: This is an optional step, and only required if the DNS server was not configured earlier, or you had configured the appliance node host name, or you want to change the previous DNS configuration. Ensure that the configured DNS server can resolve the eth1 IP address to a valid node host name as this is required for AutoSupport CallHome to work correctly.

---

19 Enter the DNS server domain name.

20 Enter the IP address for the private network.

The private network can be any IPv4 address that does not conflict with the provided management or data network ranges.

Note: The base network IP address is calculated by using the netmask that is specified for the private network, and the IP addresses are assigned starting from this base IP address. The first IP address is reserved for the NLM (Network Lock Manager) service and successive IP addresses are assigned to the network interfaces.

---

21 Enter the netmask for the private IP address.

The netmask is used to customize the private IP range. The netmask must be 255.252.0.0 or greater.

22 To configure the cluster in lockdown mode, enter **yes**.

If you opted to configure the cluster in lockdown mode, specify the following options:

- Lockdown mode: The lockdown mode creates Write Once Read Many (WORM) storage that prevents your data from being encrypted, modified,

or deleted. You can specify enterprise or compliance mode, with compliance mode providing the highest level of data security.

- Minimum retention period: The minimum duration in seconds, hours, days, weeks, months, years, for which to retain the data. The minimum retention period is 1 hour.
- Maximum retention period: The maximum duration in seconds, hours, days, weeks, months, years, for which to retain the data. The maximum retention period is 60 years.

You can also change the lockdown mode after the cluster is configured. For details, see the *Veritas Access Appliance Administrator's Guide*.

23 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. During the configuration, disk-based fencing is configured. You cannot change the fencing configuration.

The URL to access the Access web interface is displayed during the configuration.

The appliance is restarted to bring up the Access services as part of the configuration process. After the configuration is complete, a summary of the cluster configuration is displayed.

24 Change the known default password of the admin, maintenance, and IPMI (if the sysadmin account uses the default password) user accounts.

Veritas enforces changing the known default passwords during the initial configuration to ensure that the default passwords do not remain active on the node.

Ensure that the following password requirements are met:

- The password cannot reverse the entire user name.
- The password must contain at least eight characters.
- The password must contain at least one numeric character (0-9).
- The password must contain at least one lowercase character (a-z).
- The password must contain at least one uppercase character (A-Z).
- The password must contain at least one special character (~!@#$%^&).

Note: The maintenance user password must be the same on each node. If the password expires, log in to the Access web interface with the maintenance account to change the password.

After the configuration is complete, you can log in to the appliance using any of the following user interfaces:

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 6.

Chapter 4

Getting started with the Veritas Access GUI

This chapter includes the following topics:

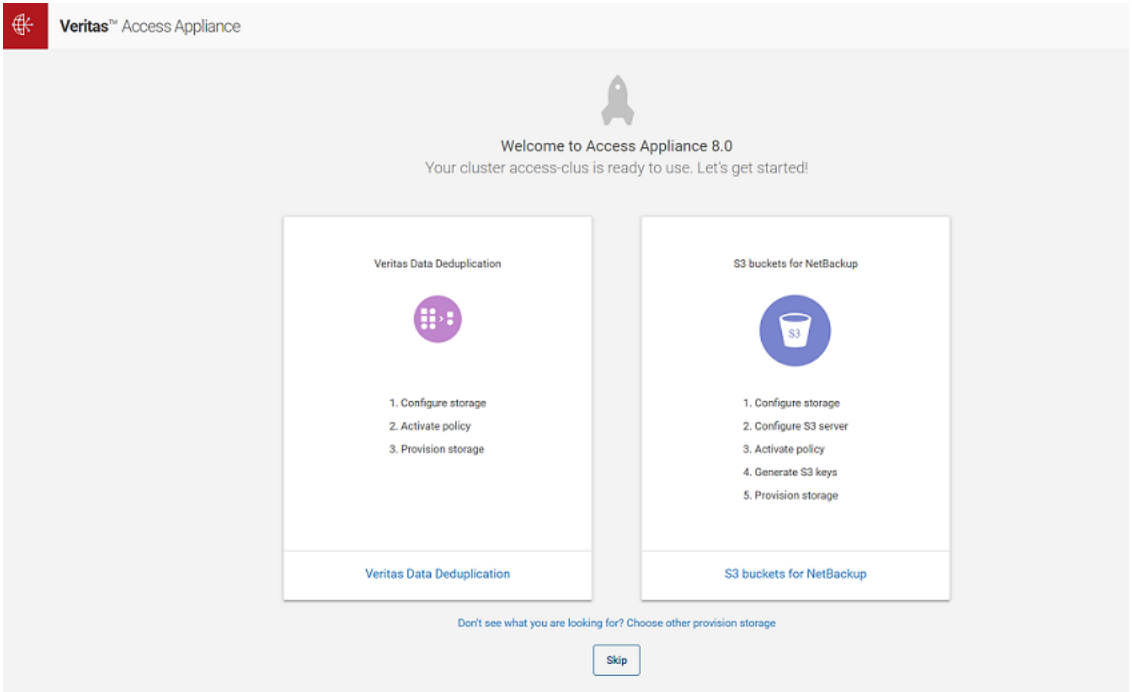
Accessing the Veritas Access web interface

You can access the Veritas Access web interface (UI) at `http://console-ip:14161` where *console-ip* is the management console IP address where the web interface is hosted. The URL to access the UI is displayed during the initial configuration.

The URL to access the UI is also displayed when you log in to the Veritas Access command-line interface using the `ssh admin@consoleIP` command.

You can use the UI to configure storage and manage your Veritas Access environment.

When you log in to the Veritas Access UI for the first time after the cluster is configured, the following screen is displayed:



You have the option to provision storage or go directly to the **Dashboard**. You can provision storage for Veritas Data Deduplication, for S3 buckets for NetBackup, or you can click the link to view more options for provisioning storage.

If you want provision storage later and instead go to the **Dashboard**, click **Skip**. The **Dashboard** provides an overview of the cluster configuration and its components and services. From the **Dashboard** you have multiple options to provision storage:

- At the top of the screen, click **Provision** where notification about storage not provisioned is displayed.
- In the **Provisioned Storage** area, click **Provision**.
- At the top of the page, click the **Provision storage** icon.

Chapter 5

Network connection management

This chapter includes the following topics:

Configuring network address settings on the appliance nodes

You can configure the network settings for the eth1 network interface of an appliance node. If eth1 is already configured, the new network settings overwrite the earlier network configuration. You cannot change the configuration from the Appliance Shell Menu when the node is already a part of the cluster.

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

See "About IPv4-IPv6-based network support on the Access Appliance" on page 41.

To configure the appliance node to communicate with one network:

1. Log on to the Access Appliance shell menu on the desired node.
2. Enter the following command to verify which network ports and bonds are plugged and available for configuration:

   ```
   show network interface
   ```

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

   ```
   set network interface ip=ipaddress netmask=netmask
   gateway=gateway-ipaddress
   ```

   - **ipaddress**: The new IPv4 address that you want to assign to the network interface.
   - **netmask**: The subnet mask (IPv4) or prefix length (IPv6).
   - **gateway-ipaddress**: The default gateway for the appliance node.

   ip, netmask, and gateway are required parameters.

   For example:

   ```
   set network interface ip=10.180.2.3 netmask=255.255.255.0
   gateway=10.180.2.1
   ```

   Note: You should not use both IPv4 and IPv6 addresses in the same command. For example:

   ```
   set network interface gateway=1.1.1.1 ip=9ffe::9
   netmask=255.255.255.0
   ```

See "About NIC1 (eth0) port usage on the appliance nodes" on page 41.

Deleting network settings on appliance nodes

You can delete network settings configured for the eth1 network interface of the appliance nodes. You cannot change the configuration from the Access Appliance shell menu when the node is already part of the cluster.

1. Log on to the Access Appliance shell menu of the node.
2. Enter the following command:

   ```
   delete network interface
   ```

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.

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 39.

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 assign either an IPv4 or an IPv6 address to the eth0 and eth1 interface.

Consider the following points for IPv6 addresses:

- You can configure a pure IPv6 network for the appliance. An IPv6 address can be configured for the appliance node management interface (eth1). However, Call Home is not supported in a pure IPv6 network configuration.
- 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, do no use `set network interface gateway=1.1.1.1 ip=9ffe::9 netmask=255.255.255.0`.
- 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 IPv6 address for a network interface card (NIC).
- Network File System (NFS) or Common Internet File System (CIFS) protocols are supported over an IPv4 network on the appliance.

- You can add an IPv6 address using the `set network interface` command. This command can only be run on a node that is not a part of the cluster. The `set network interface` command can set only the eth1 network interface.

See "Configuring network address settings on the appliance nodes" on page 39.

Configuring VLAN settings on the appliance nodes

You can configure the VLAN settings for the eth1 network interface of an appliance node. Only one VLAN can be configured for the eth1 management network interface. You cannot change the settings from the Access Appliance shell menu when the node is a part of the cluster.

1. Log on to the Access Appliance shell menu of the node on which you want to configure the settings.
2. Enter the following command to configure the VLAN settings:

   `set network vlan gateway=`*`gateway-ipaddress`* `ip=`*`ipadddress`* `netmask=`*`netmask`* `vlanid=`*`vlanid`*

   - **ipaddress**: The new IPv4 address that you want to assign to the network interface.
   - **netmask**: The subnet mask (IPv4) or prefix length (IPv6).
   - **gateway-ipaddress**: The default gateway for the VLAN.
   - **vlanid**: VLAN identifier [1-4095]

   ip, gateway, netmask, and vlanid are required parameters.

For example, `set network vlan gateway=10.182.1.1 ip=10.182.20.255 netmask=255.255.224.0 vlanid=340`

Note: Do not use both IPv4 and IPv6 addresses in the same command. For example:

`set network interface gateway=1.1.1.1 ip=9ffe::9 netmask=255.255.255.0 vlanid=340`

Viewing VLAN settings

You can view the properties of the VLAN that is tagged to the eth1 network interface.

1. Log on to the Access Appliance shell menu of the node on which you want to view the settings.
2. Enter the following command:

   ```
   show network vlan status
   ```

Deleting a VLAN

You can delete the VLAN that is tagged to eth1 network interface. If the node is already a part of the cluster, you cannot change the configuration from the Access Appliance shell menu.

1. Log on to the Access Appliance shell menu of the node.
2. Enter the following command:

   ```
   delete network vlan vlanid=vlanid
   ```

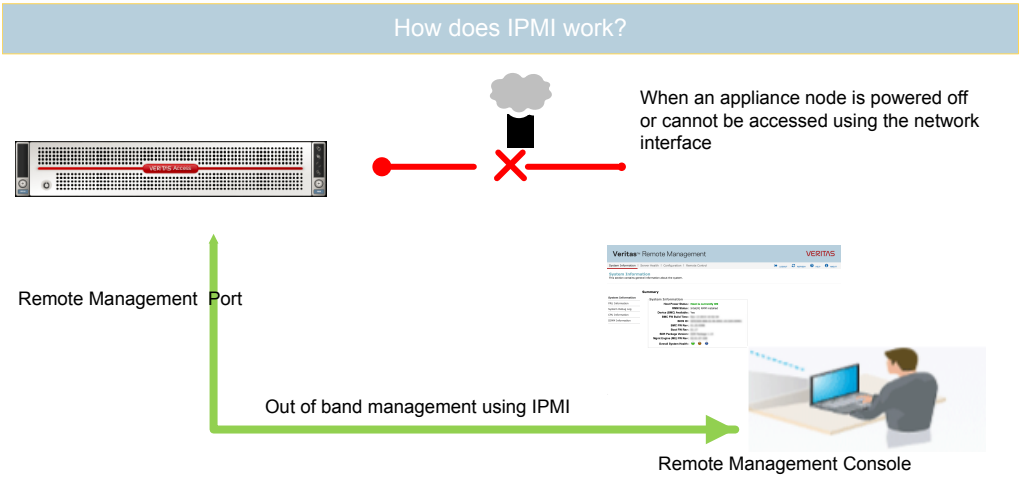
   where *vlanid* is the VLAN identifier [1- 4095]

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 5-1 Diagram of how IPMI works



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. Enter the `system ipmi network ip= netmask= gateway=` command.

   where ip is the new IP address for the IPMI port. The netmask 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 `system ipmi network show` command to view the IPMI network details
4. Type `Exit` and press Enter to log out of the Access Appliance shell menu.
5. 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 46.

See “Managing IPMI users on an appliance node” on page 45.

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. Enter the system ipmi user add=*username*

   where *username* is the new user that you want to add.
3. When prompted, enter and confirm the password for the new user:

```
New password: password
Confirm password: password
Operation completed successfully
```

To view the Veritas Remote Management Console users

1. Log on to the Access Appliance shell menu.
2. Enter the `system ipmi user show` command.

```
[access-8.0] node-01 > system ipmi user show
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. Enter the `system ipmi user delete=`*`username`* command.

   where *username* is an existing user that you want to delete.

```
[access-8.0] node-01 > system ipmi user delete=user01
User user01 has been deleted successfully.
```

See “Resetting the IPMI on an appliance node” on page 46.

See “Configuring the IPMI port on an appliance node” on page 45.

Resetting the IPMI on an appliance node

If the Veritas Remote Management Console stops responding, you can reset it using the `system ipmi reset` command.

To reset the IPMI

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

   ```
   system 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 45.

See “Managing IPMI users on an appliance node” on page 45.

Chapter 6

Monitoring the appliance

This chapter includes the following topics:

About hardware monitoring in the Access GUI

See "Testing the appliance hardware" on page 53.

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.

Note: Call Home is not supported in a pure IPv6 network configuration.

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 49.

Setting up AutoSupport on the appliance

Table 6-1 lists the steps that you need to carry out to set up AutoSupport for the appliance.

Table 6-1 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 49.
Step 2	Configure Call Home settings on the appliance. **Note:** See "To enable Call Home on the appliance" on page 50.Call Home is enabled by default.

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. If the appliance is configured to use a proxy server, configure the proxy server.

   See "Using a proxy server with the appliance" on page 50.
3. Configure the SMTP server.

   See "Setting up email notifications on the appliance" on page 51.
4. Set up email notifications.

   See "Setting up SNMP notifications on the appliance" on page 52.

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)
- Download software updates from Veritas website.

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. Enter the `set proxy-server settings server= tunnel= user=` command.

- *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`).
- *[user]*: Type the appropriate user name if the proxy server requires authentication. You are prompted for a password after you execute the command.

See "About Veritas AutoSupport on the Access Appliance" on page 48.

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. Enter the following command to set the SMTP mail server:

   ```
   set alerts email-smtp smtp-server= smtp-account=
   ```

   where **smtp-server** is the IP address or FQDN of your SMTP mail server and **smtp-account** is name of the user account that is used to access the SMTP server.

   When prompted, enter the password for the user name if authentication is required to access the SMTP account.
3. Enter one or both of the following commands to set the email addresses that you want the appliance to send emails to:

   ```
   set alerts email-hardware email-address=
   ```

   ```
   set alerts email-software email-address=
   ```

   where **email-address** is the email address of the appliance hardware administrator and the email address of the appliance software administrator.

Note: Separate multiple email addresses using a semi-colon (;). Do not add a space before or after the semi-colon.

---

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

```
set alerts email-sender-id email-address=
```

where **email-address** 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:

```
set alerts email-notification-interval interval=
```

where **interval** is the time interval in minutes.

6 Tto verify the appliance email notification settings, enter the following command:

```
show alerts email
```

See "Setting up SNMP notifications on the appliance" on page 52.

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 or the SNMPv3-SMI application protocol to monitor the appliance.

To configure SNMP notifications

1. Log on to the Access Appliance shell menu.
2. To set the SNMP server, enter the following command:

   ```
   set alerts snmp server= port=
   ```

   ```
   set alerts snmp community=
   ```

   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 **port** and **community** parameters.

   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:

   ```
   show alerts snmp mib
   ```

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

See "Setting up email notifications on the appliance" on page 51.

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. Type the `system self-test hardware` command.

   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 `system self-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.

Chapter 7

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 the appliance to a clean unconfigured factory state. The appliance is reset to its default factory settings and to the version that was installed at the factory. By default, a factory reset discards all storage configuration and data. When you initiate the factory reset, you can choose to retain the network configuration. In addition, you can specify whether to restart the appliance after the factory reset completes. Veritas recommends that you choose to automatically restart the appliance to avoid restarting the appliance manually. The appliance must be restarted after the factory reset operation.

When a node is in a cluster, the factory reset operation resets both the cluster nodes. You can factory reset both the cluster nodes without having to remove the nodes from the cluster. Additionally, during the factory reset operation, you can choose to erase data from the disks. If the node is not in a cluster, the factory reset operation resets the node and all the data on the shared storage is preserved.

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

- Appliance operating system
- Appliance software
- Access software
- Storage configuration and data

- Network configuration (optional)
- Disk erasure (optional)

Performing factory reset for cluster nodes

Use this procedure when the nodes are in a cluster and you want to factory reset both the cluster nodes. When you initiate a factory reset, both the cluster nodes are reset to their default factory settings and to the version that was installed at the factory. The password is set to its original known default value. During the factory reset process, you can choose to erase data from the disks. If you choose to erase the data, the data disks are overwritten with a digital pattern in 1, 3, or 7 passes.

To perform factory reset, you log on to one of the nodes in the cluster. This node establishes an SSH connection with the other node in cluster and initiates the factory reset operation on the other node with the configured network and storage settings. The first node waits until the factory reset operation is completed successfully on other node in the cluster before beginning the same process on the first node. If the factory reset fails to complete because of any error on the other node, the factory reset operation is terminated.

You cannot factory reset the appliance if the appliance is in lockdown mode or if the upgrade is ongoing.

To factory reset the cluster:

1. Using SSH, log on to the Access Appliance shell menu of one of the nodes in the cluster.
2. Enter the `system factory-reset` command.
3. Confirm that you want to continue with the factory reset operation and reset both the nodes in the cluster.
4. Specify whether you want to reset the network configuration. If you enter no, the DNS and IP configuration information is retained. The host name is reset to its default irrespective of whether you choose to delete or retain the network configuration. If you enter yes, the network configuration is deleted.
5. Specify whether you want to erase the data disks. If you choose to perform disk erasure, specify the number of times to overwrite the disks with a digital pattern.

   The nodes are restarted automatically after the factory reset is complete if you erase the disks.
6. If you choose not to erase the disks, specify whether you want to restart the nodes after the factory reset is complete. Veritas recommends that you choose to restart the nodes automatically after the factory reset operation is complete.

7 Review the selected options and the summary of changes.

The following message is displayed. If you want to begin the factory reset operation, enter **yes**.

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

8 The factory reset process starts and the following messages are displayed if you opted to erase the disks:

```
The appliance factory reset process is running as a background
task.
To check the current status, run the 'system factory-reset status'
 command.
```

You can monitor the status and view the task details on the status screen or press Ctrl + C to exit the current session without terminating the factory reset process. You can continue to monitor the status using the `system factory-reset status` command.

If you chose not to erase the disks, you cannot terminate the current session using Ctrl +C.

Chapter 8

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

When the STIG option is not enabled, the following password requirements must be met:

- The password must contain at least eight characters.
- The password must contain at least one lowercase character (a-z), uppercase character (A-Z), numeric character (0-9), and special character (!#$%&+,-.<=>@[]^_{|}~).
- The password cannot be a dictionary word.
- The last seven passwords cannot be reused, and the new password cannot be similar to the previous passwords.

When the STIG option is enabled, the following password requirements must be met:

- The password must be at least 15 characters long and must include at least one character from the following categories:
  - Numbers
  - Lowercase characters
  - Uppercase characters
  - Special characters (!#$%&+,-.<=>@[]^_{|}~)
- The password can contain a maximum of two consecutive repeating characters.
- The password can contain a maximum of four consecutive repeating characters from the same category.

- The password must contain a minimum number of eight different characters.
- The password must be retained for a minimum of 1 day before changing it.
- The password must be changed after a maximum of 60 days.
- The password cannot be a dictionary word.
- The last seven passwords cannot be reused.
- The new password must have at least 8 characters that are different from the old password.

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.

About forced password changes

For increased security, forced password changes are enforced during the initial cluster configuration to ensure known default passwords do not exist on the system.

You must change the default passwords for the admin, maintenance, and IPMI user accounts. The GRUB and root passwords are set to the maintenance account password.

When you change the password, the changed password is synchronized with the other node in the cluster. If after three attempts you fail to change the password, you are prompted to change the password the next time you log in to the node.

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 elevate` 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.

You must change the default password during the initial configuration process. If you fail to change the password after three failed attempts, you can change the default password using the Access web interface (UI) or the command-line interface. If STIG is enabled and the password expires, use the Access UI to change the password.

After the cluster is configured successfully, the appliance does not support setting the Maintenance password by using commands such as `Password maintenance`.

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 62.

See "Auditing the SDCS logs on an Access Appliance" on page 62.

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 61.

See "Auditing the SDCS logs on an Access Appliance" on page 62.

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. Enter the following command:

```
show sdcs-audit search
```

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. (Optional) Enter the following command to view all of the events that occurred on a specific day:

   `show sdcs-audit view search to-date=`*`date`*

   where *date* is the day in the `mm/dd/yyyy[-hh:mm:ss]` format.
3. (Optional) Enter the following command to view all of the events that occurred during a specific period of time:

   `show sdcs-audit search to-date=`*`todate`*`fromdate=`*`from-date`*

   where *todate* is the end date and *fromdate* is the start date.

   For example: `show sdcs-audit search to-date=08/31/2021 from-date=08/21/2021`

To filter SDCS log events by severity

1. Log on to the Access Appliance shell menu.
2. Enter the `show sdcs-audit search severity=`*`severitycode`* `command.`

   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 65.

To filter SDCS log entries by type

1. Log on to the Access Appliance shell menu.
2. Enter the `show sdcs-audit search event-type=`*`eventtype`* command.

   where *eventtype* 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 65.

Filter using multiple attributes

You can filter the security logs based on multiple attributes.

To search based on multiple attributes

1. Log on to the Access Appliance shell menu.
2. Enter the `show sdcs-audit search event-id=`*`eventid`* `event-type=`*`eventtype`* `from-date=`*`fromdate`* `to-date=`*`todate`* `severity=`*`severitycode`* `search-string=`*`text`* command.

   where

   - *eventid* is the audit log event ID
   - *eventype* is 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..
   - *fromdate* is the start date.
   - *todate* is the end date.
   - *severitycode* is 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.
   - *text* is the search term.

   For example:

   ```
   show sdcs-audit search event-type=MSTA severity=I
   to-date=08/31/2021 from-date=08/21/2021
   search-string=retranslation
   ```

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. Enter the `show sdcs-audit search event-id=eventid`command.

   where *eventid* 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 61.

See “Reviewing SDCS events on the Access Appliance” on page 62.

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

Table 8-1 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	
N	Notice	A more serious event than Warning, but less serious than Critical. 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:

```
show sdcs-audit view severity-codes
```

Table 8-2 SDCS event codes

Code	Description
DAUD	IDS Audit
DFWU	File Watch Unix
DFWW	File Watch Windows
DGEN	Generic Log
DIPS	IPS to IDS Event

Table 8-2 SDCS event codes *(continued)*

Code	Description
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
PREG	IPS Registry

Table 8-2 SDCS event codes *(continued)*

Code	Description
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

```
show sdcs-audit view event-type-codes
```

See "Auditing the SDCS logs on an Access Appliance" on page 62.

Changing the SDCS log retention settings on an Access Appliance node

By default, the Access 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 `show sdcs-audit settings` command.

To change the SDCS log retention settings

1. Log on to the Access Appliance shell menu.
2. To set the number of days in the retention period:

   `set sdcs-audit settings retention-period=`*`days`*

   where *days* is the specific number of days that you want the appliance to retain each log entry.
3. To set the number of log files the appliance retains:

   `set sdcs-audit settings file-number=`*`number`*

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

About the Access Appliance intrusion prevention system

The appliance intrusion prevention system (IPS) consists of a custom Symantec Data Center Security (SDCS) policy that runs automatically at startup. The IPS policy can proactively block unwanted resource access behaviors.

The following list contains some of the IPS policy features:

- Restricted access to the root account by maintenance user.
- Self-protection for the SDCS agent itself to ensure that the security features and monitoring features of SDCS are not compromised.

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).

The following table lists the software products that were used to scan the Access appliance.

Table 8-3 Security scanners used for testing Veritas Access appliances

Security scanner	Version
Nessus™	8.14.0
QualysGuard™	12.2.62

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.
- Use Access Control Lists (ACLs) or isolated networks to limit access to the IPMI interface.

Login

Table 8-4 Login security settings

Settings	Recommended values
Failed login attempts	3
User Lockout time (min)	60 seconds
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 8-5 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.