

[All content](#)[Search here](#)

[Compass](#) › [Products](#) › [Connectors](#) › [IdentityNow Connectors](#)  
› [Virtual Appliance Reference Guide](#)

[Options](#)

# Virtual Appliance Reference Guide



A virtual appliance (VA) is a Linux-based virtual machine that connects to your sources and apps using APIs, connectors and integrations already available from SailPoint.

This document contains system and network requirements, an overview of the deployment workflow, monitoring and maintenance information, and links to other documents about planning, best practices, deployment, configuration, and troubleshooting.

See the following sections for information:

- [About the SailPoint VA](#)
- [VA Deployment and Configuration](#)
- [System and Network Requirements](#)
  - [Network Considerations](#)
- [Monitoring and Maintenance](#)
  - [VA Updates](#)
  - [Monitoring Your VA Infrastructure](#)
  - [Maintaining Your VA Infrastructure](#)

## About the SailPoint VA

Each SailPoint VA is deployed on your infrastructure, and managed by SailPoint. After the VA image is deployed successfully behind your firewall, it is your responsibility to keep your VA(s) operational by performing regular monitoring and maintenance.

While SailPoint doesn't connect directly to the VA, each VA must be able to make continuous outbound-only calls to the cloud environment to execute actions such as installing patches and updating images. We also have monitoring built in to alert us when a VA goes down.

**NOTE:** Adding users, VA trust/key store access, and root access are not supported.

## VA Deployment and Configuration

Because the VA is critical to your SailPoint infrastructure, you'll need to understand your options, make crucial deployment and configuration decisions, and carefully complete installation.

Complete the following steps to get a VA up and running:

### 1. Understand VA Options and Requirements

Read the following documentation to understand your options and requirements before proceeding:

- Virtual Appliance Planning and Best Practices
- System and Network Requirements
- Deploying the Virtual Appliance with IdentityIQ – IdentityIQ customers must follow instructions this documentation. Deploying the VA with IdentityIQ requires adding `product: iai` to the `va-config-<va_id>.yaml` file.

### 2. Choose a Deployment Type

You can deploy the VA image to the following virtualization platforms:

- **Local with vSphere** – Deploy the downloaded image on a virtual machine behind your firewall. Local deployments require a static

network.

- **Local with Hyper-V** – Deploy the downloaded image on a virtual machine behind your firewall. Local deployments require a static network.
- **AWS Cloud** – Deploy our AMI on your AWS infrastructure.
- **Azure Cloud** – Deploy the downloaded image on a virtual machine running in your Azure environment.

### 3. Choose a Network Configuration

You can choose from the following network configuration options:

- **Standard** – Uses the standard traffic generated by the VA.
- **HTTP Proxy** – Routes all HTTP/HTTPS traffic through a proxy.
- **Secure Tunnel** – Strictly limits the outbound connections generated by the VA.

In addition to the primary configurations above, you can add TLS encryption, a proxy server for the Password Interceptor, or use a local NTP server.

### 4. Complete Deployment

Refer to the documentation for your selected virtualization platform and complete all prerequisites and steps.

### 5. Complete Configuration

Refer to the documentation for your selected network configuration and complete all prerequisites and steps.

### 6. Monitor and Maintain the VA

See the section on Monitoring and Maintenance for information on how to ensure the health of your VA.

## Troubleshooting

We're confident that after you successfully complete the deployment and configuration process, your VA will be fully operational. If you experience any problems, please see the Virtual Appliance Troubleshooting Guide for help.

## System and Network Requirements

Virtualization Environments			
Local	vSphere 6.5+  Microsoft Hyper-V Server 2016, Windows Server 2016		
Cloud	AWS  Azure		
VA Image Sizes			
Local	<b>Minimum</b> Processor: 1 Memory: 8 GB Storage: 128 GB	<b>Recommended</b> Processors: 2 Memory: 16 GB Storage: 128 GB	<b>IdentityIQ Users With AI Services</b> Processors: 4 Memory: 16 GB Storage: 128 GB
AWS EC2 Instance Size	m4.large  See Amazon EC2 Instance Types for details.		
Azure VM Instance Size	Standard_B2ms		
VA Locations and Minimum Distributions			
Virtual Machines	1 VA per 1 virtual machine host		
Clusters	2 VAs minimum per cluster to ensure connectivity during updates		

VAs and Sources	<ul style="list-style-type: none"> <li>Local – Each cluster should be installed in close proximity to the connected source system.</li> <li>AWS/Azure – Each cluster should be placed in the Availability Zone as close as possible to the target sources. If your organization has a VPN connection to its AWS or Azure VPC, the VAs should be hosted in the same regions hosting the network gateways for your organization.</li> </ul>
Sandbox	2 VAs minimum on your Sandbox cluster
High Availability and Disaster Recovery	2 VAs minimum. A load balancer is not required.
DMZ	DMZ deployment should be avoided.
<b>Network Requirements</b>	
Ports	<p>Outbound access for port 53 (DNS) to your internal name servers</p> <p>Outbound access for ports 123 (NTP) and 443 (HTTPS). If you connect all of your VAs to local NTP servers, you can close port 123.</p> <p>Optional inbound access for port 22 (SSH) for you to access the VA when inside your network</p> <p><b>NOTE:</b> Target systems might have their own port requirements. VAs must be allowed to communicate over the ports they require.</p>
Deep Packet Inspection	Not supported
Third-party Monitoring	Not supported
DNS Servers	Required. VAs must connect to your internal DNS servers. You can connect VAs to a local DNS server behind your firewall.
NTP Servers	Required. VAs must connect to a network time protocol (NTP) server. You can connect VAs to a local NTP server behind your firewall.
HTTP Proxy Servers	Optional. You might have to allow access to URLs for external sources and tools.
Secure Tunnel	Optional. VA traffic must be allowed access to primary and region-specific AWS URLs

## Network Considerations

## Allowing VA Traffic to URLs

Network proxy, security, firewall, or caching products such as Websense can interfere with the VA. To avoid this problem, all outbound traffic to any destination must be allowed, through the ports specified in the network requirements.

See [Allowing VA Traffic to URLs](#) for the list of URLs that the VA must be able to reach.

## HTTP Proxy

SailPoint virtual appliances can be optionally configured to use a network proxy. In this case, all HTTP/HTTPS traffic (such as virtual appliance communication and updates) is routed through the proxy. Traffic for all sources connecting to *internal* endpoints *is not* routed through the proxy.

Traffic to external sources such as Salesforce, Box, ServiceNow, Office365, GoogleApps, GoToMeeting, WebEx, and Workday is also routed through the proxy. You may be able to allow traffic to these external sources; consult your network administrator for more information.

The connection from the VA to the proxy can be authenticated only if your proxy supports basic authentication over the connection string. If not, the connection must be unauthenticated. We do not currently support other authentication mechanisms, however, you may add IP address source to the allow list.

## Connecting the VA to a Local NTP Server

By default, virtual appliances are configured to communicate with external network time protocol (NTP) servers using port 123. If you do not want to allow outbound access for port 123, you can configure your virtual appliances to communicate with NTP servers behind your firewall.

Each virtual appliance must be configured individually. While you do not have to configure every virtual appliance to use your NTP server, you cannot close port 123 until all of your virtual appliances have been configured to use internal NTP servers.

Complete the following steps:

1. Edit the `timesyncd.conf` file using the full path:

```
sudoedit /etc/systemd/timesyncd.conf
```

2. Add entries to the NTP line for local servers using the server host names or IP addresses. More than one server can be added, separated by a space.

Examples:

```
NTP=chronos.acme.com
```

```
NTP=chronos1.acme.com chronos2.acme.com
```

**CAUTION:** Be sure to remove the `#` sign on the NTP line before adding server names.

3. Save the changes to the `timesyncd.conf` file.

4. Restart the `systemd-timesyncd` daemon:

```
sudo systemctl restart systemd-timesyncd
```

5. To check the UTC time status on the VA use the following command:

```
timedatectl status
```

## Monitoring and Maintenance

Virtual appliances are connected to a variety of resources in your SailPoint environment to support secure communication between SailPoint and your systems. It's therefore important to regularly monitor and maintain each SailPoint VA, and be familiar with all of the connected sources.

See the following sections for information:

- VA Updates
- Monitoring VAs
- Maintaining Your VA Infrastructure

## VA Updates

SailPoint manages VA updates. Whenever we make improvements to the VA image, we deploy them to the clusters, which then perform rolling updates and reboots on the related VAs. Having at least two VAs per cluster ensures connectivity with your sources during these updates. By applying updates and rebooting one at a time, the VA cluster maintains full availability during the update process.

**CAUTION:** If any VA in a cluster is down, no software or maintenance updates are made to any of the VAs in that cluster.

## Monitoring Your VA Infrastructure

SailPoint has monitoring built in to alert us if a VA goes down. We do not allow external monitoring of VAs.

It is important for you to regularly monitor the health of your VAs and be familiar with the connections between VAs and sources.

The following sections provide instructions for these tasks:

- Monitoring VA Health
- Reviewing the VAs Connected to a Source
- Reviewing the Sources Connected to a VA

### Monitoring VA Health

You have the following options to check on the health of your VAs:

- **Notifications** – You can configure IdentityNow to send you email when a VA goes down.
- **Admin Dashboard** – Click the Clusters tile of the system components status panel.
- **Virtual Appliance Clusters page** – Click **Admin > Connections > Virtual Appliances** to see the status of your VA clusters. Click on a cluster name and select **Virtual Appliances** to see the status of that cluster's VAs. See this section of the Troubleshooting Guide for descriptions of each status.

### Reviewing the VAs Connected to a Source




Complete the following steps to review the VAs connected to a specific source:

1. In the Admin interface, click **Connections > Sources**.
2. Click the source you want to review.
3. Click the **Connections** tab. The VA cluster connected to the source is displayed under **Virtual Appliance**.
4. Click the cluster name to view more details about the cluster.

## Reviewing the Sources Connected to a VA

Complete the following steps to review the sources connected to a specific VA:

1. In the Admin interface, click **Connections > Virtual Appliances**.
2. Click the cluster name you want to review.
3. Click the **Connections** tab. The names of all sources connected to the cluster and what they are used for are displayed.
4. To make changes to a source connection, click the Edit icon  for the source.

## Maintaining Your VA Infrastructure

Maintaining your VA infrastructure ensures continuous connectivity with your sources. If there is an issue with a VA, it is important to respond quickly so the VAs are available for updates and able to maintain connectivity.

The following sections provide instructions for tasks you may have to perform as part of VA maintenance:

- Resetting your VA Password
- Adjusting VAs for Daylight Saving Time
- Verifying the OS of Your VA Image
- Deleting a VA Cluster
- Deleting a VA
- Recovering from a VA Failure

## Resetting your VA Password

You can change the password on each VA at any time. Complete the following steps:

1. Sign in to the virtual machine on which the VA is running.
2. At the command prompt, type `passwd`
3. Enter the current password.
4. Enter the new password.
5. Repeat the new password.
6. Reboot the VA: `sudo reboot`

## Adjusting for Daylight Savings Time

The time zone used for a direct source's aggregation scheduling is read from the VA cluster time zone. VA system clocks do not automatically change for Daylight Savings Time (DST). For this reason, if your organization is in a region that observes this yearly time change, and you want your system to perform aggregations at the same time all year, you will need to adjust the cluster time zone (GMT offset) at the beginning and end of DST.

### Example:

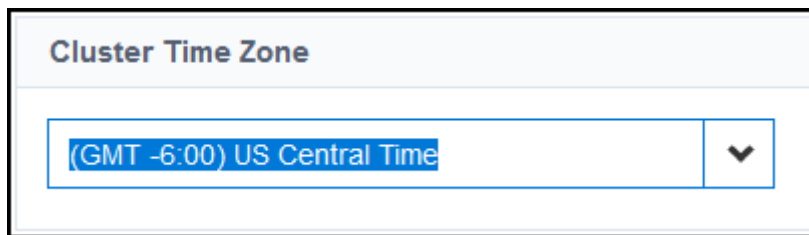
Your organization is in the Central Time Zone and has scheduled direct source aggregations to run at 4:00 a.m. When DST begins, other clocks change, but the VA cluster time does not. During DST, your aggregations will therefore run at 3:00 a.m. even though they are scheduled on your source to run at 4:00 a.m.

To keep your aggregations running at 4:00 a.m., you must change the VA cluster time zone from (GMT -6:00) Central Time to (GMT -5:00) Eastern Time at the beginning of DST. Then, at the end of DST, you must change the VA cluster time zone back to (GMT -6:00) Central Time.

Complete the following steps to change a VA cluster time zone:

1. In the Admin interface, click **Connections > Virtual Appliances**.

2. In the list of virtual appliance clusters, click the cluster you want to change.
3. In the Cluster Time Zone panel, select the desired GMT offset from the drop-down menu.



The screenshot shows a panel titled "Cluster Time Zone". Inside the panel is a dropdown menu. The selected option in the dropdown is "(GMT -6:00) US Central Time". A small downward arrow icon is visible to the right of the text in the dropdown.

4. Click **Save**.

## Verifying the OS of Your VA Image

If you're not sure which version of the VA you're currently using, run the following command:

```
uname -a
```

Look for `<x.x.x>-flatcar` in the results.

Where:

`<x.x.x>` is the VA version number

`flatcar` is the VA OS

**NOTE:** If your results return `coreos`, your VA image is not using the latest, supported OS.

## Deleting a VA Cluster

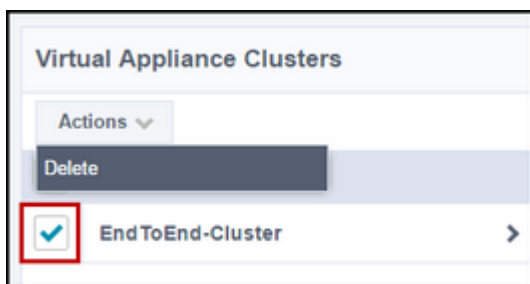
Deleting a VA cluster deletes every VA associated with that cluster.

**NOTE:** You cannot delete a virtual appliance cluster while it is connected to a source. You must remove the connection first. See reviewing the Sources Connected to a VA.

**Complete the following steps to delete a VA cluster:**

1. In the Admin interface, click **Connections > Virtual Appliances**.

2. In the list of virtual appliance clusters, select the cluster you want to delete.
3. Click **Actions** and select **Delete**. This will delete all virtual appliances in the selected cluster.



4. In the confirmation window, click **Continue**.

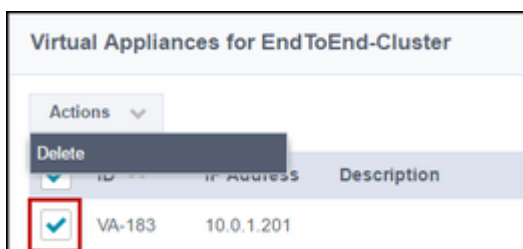
A confirmation message notifies you that the VA cluster has been deleted, and the deleted cluster is removed from the cluster list.

## Deleting a VA

You can delete a VA without deleting the entire cluster, to replace a single VA with a new one.

### Complete the following steps to delete a specific VA:

1. In the Admin interface, click **Connections > Virtual Appliances**.
2. In the list of virtual appliance clusters, click the cluster that includes the VA you want to delete.
3. Click **Virtual Appliances** and select the checkbox next to the VA you want to delete.
4. Click **Actions** and select **Delete**. A success message is displayed at the top of the list of VAs.




**CAUTION:** After removing the VA from IdentityNow, you also need to shut down the related VA instances on your virtualization platform. Failure to do so can result in degraded performance or potential downtime.

## Recovering from a VA Failure

When a VA cluster fails, you need to replace it quickly with a new VA cluster and reconnect all of the sources.

### Complete the following steps to replace a failed VA:

1. Create a new virtual appliance cluster and at least two virtual appliances on that cluster.
2. Review all the sources that are connected to the failed VA.
3. In the failed VA cluster, edit sources to connect to the new VAs you just created as follows:
  - a. Click the **Connections** tab to see the list of sources connected to the failed cluster.
  - b. click the Edit icon  for each source to go directly to the source.
  - c. On the Config tab for the source, select the new cluster in the Virtual Appliance Cluster drop-down menu.
  - d. In the failed VA cluster Connections tab, repeat steps a through c until the list of Connections is empty.
4. Delete the failed VA cluster.

### Related Documentation:

- Virtual Appliance Planning and Best Practices
- Virtual Appliance Troubleshooting Guide

Virtual Appliance (VA)

aggregation

aggregation process   automatic changes on a source   daylight savings time

getting started with identitynow   identitynow va   integration with connectors

monitoring vas   ntp servers   provisioning   provisioning process

provisioning setup   testing connectivity   v2   va   va system requirements  
virtual appliance   virtual machine

Add tags



Was this article relevant?  

Comment

## COMMENTS



gsanr

Apr 29, 202

Since this information is for some reason not available in this document and took us some back and forth to find it, in case there is another lost soul looking for it:

To Shutdown a VA you have to use:

```
sudo systemctl poweroff
```

This worked on 2020-04-29 15h52 in a machine with a "uname" :

```
Linux xxx-xxxxx.xxxxxxxxxx.xxx 4.19.106-coreos #1 SMP Wed Feb 26 21:43:18 -00 2020  
x86_64 Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz GenuineIntel GNU/Linux
```



adamshaw525

Sep 24, 202

Can anyone provide technical details on how the load balancing is configured in VA clusters?

Feb 23, 202



SleepNoMore

Bump @ Adamshaw525 comment. I would also like to know more about this.



ncrai20

Mar 10, 202

Is there a limitation to the number of sources supported by VA in IdentityNow?

Currently, we have 2 VAs in our Production environment. And we have a total of 300 sources. Most of them are JDBC sources and Active Directory sources.

Thanks



vguleria

May 19, 202

Hey @ncrai20

Did you find the answer as i would also like to know about it.

Thanks.



MattUribe

Jun 15, 202

It seems odd to me that we have to manually adjust the time zone from Central to Eastern in order to adjust for Daylight Savings, especially since IdentityNow still seems to know what time it really is. Is this a limitation of the flatcar appliance?

A system that is designed to automate tasks that would otherwise be tedious and prone to being forgotten should not itself require manual tasks that may or may not be remembered when the time comes. I foresee biannual confusion when the aggregation schedules stop occurring at the expected time.

"Your organization is in the Central Time Zone and has scheduled direct source aggregations to run at 4:00 a.m. When DST begins, other clocks change, but the VA cluster time does not. During DST, your aggregations will therefore run at 3:00 a.m. even though they are scheduled on your source to run at 4:00 a.m.

To keep your aggregations running at 4:00 a.m., **you must change the VA cluster time zone from (GMT -6:00) Central Time to (GMT -5:00) Eastern Time at the beginning of DST. Then, at the end of DST, you must change the VA cluster time zone back to (GMT -6:00) Central Time.**"



darylclaudemedina

Jun 25, 202

Hello @MattUribe,

I highly suggest that you post your feedback in the SailPoint Idea Portal where you can submit ideas and vote on items you would like to see in our products. Our product managers will review the submitted ideas, and the ideas that align with our vision and strategy will automatically go into the queue for roadmap prioritization.

To find out more information on submitting ideas, please follow the step by step guide, How To: Submit an Idea. Thank you!

You can give **kudos** to replies to show your appreciation. Watch the Compass How-to Videos for more information about the community.



SHRS

Nov 09, 202

Hello @MattUribe ,



Have you raised an Idea already?

---



jgreen-calvin

Dec 07, 2021

Idea <https://ideas.sailpoint.com/ideas/GOV-I-1355> is there but has only a few votes. Please consider upvoting this item in support of automatic daylight savings handling.

---



IAMpdu

Apr 20, 2022

Hello Everyone,

Is there any way to reset VA password if we forgot the old one?

@darylclaudemedina , @MattUribe , @Justin , @Sushantmrj

Thanks,

IAM- PDU

---



edmarks

Apr 20, 2022

VA password being:

\* The sailpoint account password on a specific VA? (in this case it would probably be easiest to just create a new VA in the cluster and decommission the VA with the unknown password)

OR

\* The encrypted cluster keyphrase? (in this case a new VA cluster could be established and all sources moved to this new cluster)



Justin

Apr 20, 202

@IAMpdu,

I would agree with @edmarks comments.

Rebuilding VA's is super easy and probably the path of least resistance in this case.

Thanks!



glourenco

Thursday

Hi Guys

Is there any way to approve sailpoint updates before they are applied to the virtual appliances?

---

Comment

PREVIEW




Hint: @ links to members, content

☐ Email me when someone replies

Cancel

Post Your Comment

Version history

**Revision #:** 29 of 29  
**Last update:** Aug 10, 2022 08:29 PM  
**Updated by:** hope\_carlson 

[View Article History](#)

Contributors

  
hope\_carlson

  
kelly\_wells

[About](#) [Careers](#) [Support](#) [Trust Center](#) [Security](#) [Privacy](#) [Cookie Notice](#)  
[Terms of Use](#) [Legal](#)



Copyright © 2022. SailPoint Technologies Holdings, Inc. All Rights Reserved.