Virtual Appliance Planning and Best Practices

This document contains important considerations for planning your SailPoint virtual appliance (VA) configuration, including URLs that must be accessible for the VA to function properly, along with best practices for deploying the VA for high availability and disaster recovery. For detailed information about the VA deployment and configuration process, requirements, monitoring, and maintenance, see the Virtual Appliance Reference Guide.

See the following sections for more information:

Best Practices

SailPoint recommends the following best practices related to deploying virtual appliances:

- **Location of VAs and Sources** - To ensure a reliable connection between a VA and the source system, locate them as follows:
  - **Local** - Each cluster should be installed in close proximity to the connected source system.
  - **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 Virtual Private Cloud (VPC), the

VAs should be hosted in the same region that's hosting the network gateways for your organization.

- **Minimum Cluster Size** - To ensure connectivity during updates, we recommend you deploy ***at least 2 VAs per cluster*** because the VAs take turns updating.

- **VA to Virtual Machine Ratio** - To avoid a single point of failure in your environment, we recommend a ***1:1 ratio of VA to VM***. To build in fault tolerance, we recommend configuring local VAs in the same cluster to run on different servers whenever possible. We also recommend that VAs in the same cluster running in AWS/Azure be spread out across different Availability Zones.

- **Separate Sandbox and Production Clusters** - We recommend that you closely monitor your sandbox VA clusters and test any connectivity changes before they go to production.

- **Switching Deployment Methods** - Migrating existing VAs to a different deployment method is not supported. New VAs must be created to switch from one deployment method to another, such as from standard deployment to secure tunnel deployment.

Allowing VA Traffic to URLs

This section provides information about the URLs that must be accessible for the VA to function properly. Depending on your firewall configuration, you may need to add URLs to the allow list.

If you are required to add outbound traffic to the allow list, and your firewall does not support domain entries, we recommend you configure a secure tunnel VA.

NOTES:

- These lists are subject to change without notice.

- Deep packet inspection is not supported.

- SailPoint does not support allowing IP addresses of connected service endpoints in any configuration.

Primary URLs

The following table lists URLs that must be accessible to the VA, regardless of the VA zone.

URL	Source	Purpose
`*.flatcar-linux.net` `*.flatcar-linux.org`	Flatcar	Used for security patches and software updates
`*.identitynow.com`	SailPoint	Allows the VA to make REST requests to SailPoint
`*.sailpoint.com`	SailPoint	Allows the VA to make REST requests to SailPoint
`app.datadoghq.com`	Datadog	SailPoint uses this service to manage events sent from the VA. This gives us insight to the current configuration and behavior of the machine.
https://aws.amazon.com/s3/ `*.s3.amazonaws.com`	AWS	Required for SailPoint to communicate back to the appliance **NOTE**: Some AWS URLs are specific to the zone configured for your deployment. For information, refer to Region-Specific AWS URLs.

`api.ecr.us-east-1.amazonaws.com`
`ecr.us-east-1.amazonaws.com`
`874540850173.dkr.ecr.us-east-1.amazonaws.com`
	Elastic Container Registry	SailPoint's private container registry. Allows the VA to retrieve service updates.

NTP	N/A	Allows the clock to sync to standard **NOTE**: This is only applicable if you're using an external NTP server.

Region-Specific AWS URLs

The services in this section must be accessible, but the URLs you'll need to add to the allow list depend on the region configured for your VA. For example, SailPoint places messages into SQS in your region. The VA checks the queue for messages about work it needs to complete.

SailPoint supports the following AWS regions:

Region Name	Code
US East (N. Virginia)	`us-east-1`
US West (Oregon)	`us-west-2`
Asia Pacific (Sydney)	`ap-southeast-2`
Asia Pacific (Tokyo)	`ap-northeast-1`
Canada (Central)	`ca-central-1`
Europe (Frankfurt)	`eu-central-1`
Europe (London)	`eu-west-2`

CAUTION:

- Contact your SailPoint deployment team to determine the region you need to use.

- You must ***always*** allow:
  - The primary AWS S3 URL (`*.s3.amazonaws.com`) as noted in Primary URLs.
  - The `us-east-1` URL for each of these services, even if your region is located elsewhere.
  - The region-specific URL for each of these services if your tenant is in a region other than `us-east-1`.

The following table lists region-specific URLs that must be accessible to the VA. Replace `<region_code>` with the AWS region where your tenant resides.

Service	Region-Specific URLs to Allow
S3	https://docs.aws.amazon.com/general/latest/gr/rande.html#reg endpoints `*.s3.us-east-1.amazonaws.com` and `*.s3.<region_code>.amazonaws.com`

SQS	https://docs.aws.amazon.com/general/latest/gr/rande.html#sq `sqs.us-east-1.amazonaws.com` and `sqs.<region_code>.amazonaws.com`
DynamoDB	https://docs.aws.amazon.com/general/latest/gr/rande.html#dd `dynamodb.us-east-1.amazonaws.com` and `dynamodb.<region_code>.amazonaws.com`
Elastic Container Registry	https://docs.aws.amazon.com/general/latest/gr/rande.html#ec `874540850173.dkr.ecr.us-east-1.amazonaws.com` and `874540850173.dkr.ecr.<region_code>.amazonaws.com`
Firehose*	https://docs.aws.amazon.com/general/latest/gr/fh.html `firehose.us-east-1.amazonaws.com` and `firehose.<region_code>.amazonaws.com`

* required only for the AI Services IdentityIQ Collector

VA Configuration Options

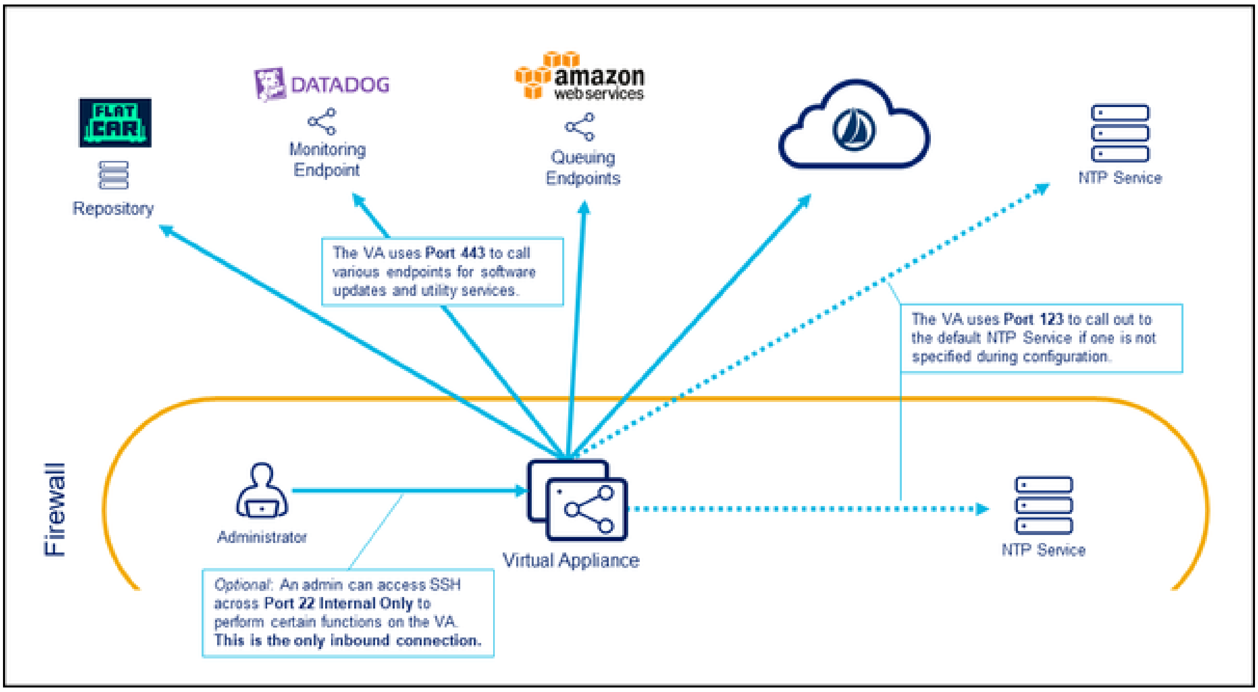
This section provides an overview of some different configuration options, along with considerations for each, to help you select and implement a configuration that will work best for you.

- Standard Configuration
- HTTP Proxy Configuration
- Secure Tunnel Configuration

Standard Configuration

Standard is the default VA configuration option, as it allows the VA to connect to SailPoint and other required endpoints directly through the firewall. There is no additional setup required to achieve connectivity after the network requirements are met.

Standard VA Configuration Diagram:


FLATCAR
Repository
DATADOG
Monitoring Endpoint
amazon webservices
Queuing Endpoints
NTP Service
The VA uses Port 443 to call various endpoints for software updates and utility services.
The VA uses Port 123 to call out to the default NTP Service if one is not specified during configuration.
Firewall
Administrator
Virtual Appliance
NTP Service
Optional: An admin can access SSH across Port 22 Internal Only to perform certain functions on the VA. This is the only inbound connection.

Considerations:

- You might have to add URLs to the allow list.
- Deep-packet inspection is not supported.

Related Documentation: Configuration Guide for Standard Virtual Appliances

Network Requirements:

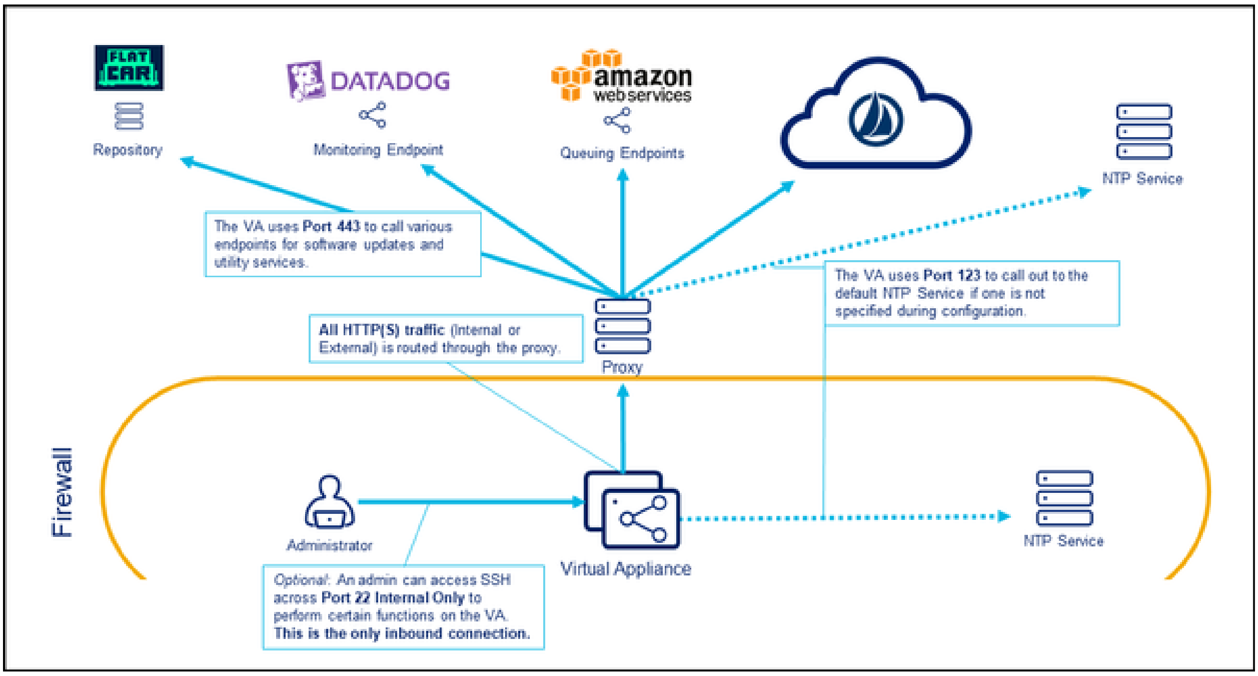
Port	Reason	Direction	IP Addresses	Description
53	DNS	Outbound	All	Used for name resolution
123	NTP	Outbound	All	Used for time synchronization. You can configure a local NTP server instead of using the default.
22	SSH	Inbound	Internal Only (Recommended)	Only required if you want to SSH into or copy files onto the VA
443	HTTPS	Outbound	All	Used for all HTTPS communication (source endpoints and/or update endpoints)

NOTE: Target systems might have their own port requirements. VAs must be allowed to communicate over the ports required by target systems.

HTTP Proxy Configuration

This configuration option requires additional setup to achieve connectivity through a previously configured proxy service. The VA connects to SailPoint and any other required endpoint through the proxy.

HTTP Proxy VA Configuration Diagram:



The VA uses **Port 443** to call various endpoints for software updates and utility services.

All HTTP(S) traffic (Internal or External) is routed through the proxy.

The VA uses **Port 123** to call out to the default NTP Service if one is not specified during configuration.

Optional: An admin can access SSH across **Port 22 Internal Only** to perform certain functions on the VA. **This is the only inbound connection.**

Considerations:

- All HTTP/HTTPS traffic (VA communication, updates, internal or external) is routed through the proxy.
- This configuration is *not* compatible with the secure tunnel configuration.
- 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, adding IP address sources to the allow list may be used.
- You might have to add URLs to the allow list.
- Deep-packet inspection is not supported.

Related Documentation: Configuration Guide for Virtual Appliance HTTP Proxy

Network Requirements:

Port	Reason	Direction	IP Addresses	Description
53	DNS	Outbound	All	Used for name resolution

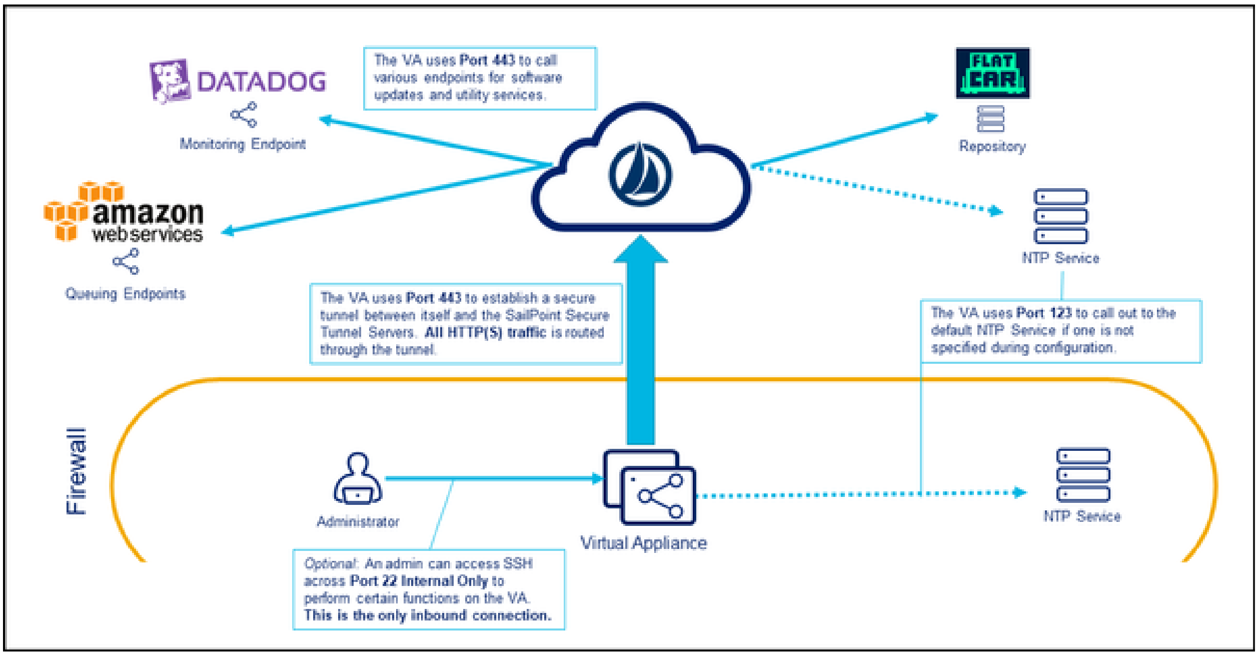
123	NTP	Outbound	All	Used for time synchronization. You can configure a local NTP server instead of using the default.
22	SSH	Inbound	Internal Only (Recommended)	Only required if you want to SSH into or copy files onto the VA
443	HTTPS	Outbound	All	Used for all HTTPS communication (source endpoints and/or update endpoints)

NOTE: Target systems might have their own port requirements. VAs must be allowed to communicate over the ports required by target systems.

Secure Tunnel Configuration

If you are required to add outbound traffic to the allow list, and your firewall does not support domain entries, we recommend using a secure tunnel configuration. This option requires additional setup for the VA to connect to SailPoint and any other endpoint through secure tunnel servers (instead of directly from the VA through the firewall or proxy).

Secure Tunnel VA Configuration Diagram:



The VA uses **Port 443** to call various endpoints for software updates and utility services.

The VA uses **Port 443** to establish a secure tunnel between itself and the SailPoint Secure Tunnel Servers. **All HTTP(S) traffic** is routed through the tunnel.

The VA uses **Port 123** to call out to the default NTP Service if one is not specified during configuration.

Optional: An admin can access SSH across **Port 22 Internal Only** to perform certain functions on the VA. **This is the only inbound connection.**

Considerations:

- All HTTP/HTTPS traffic (VA communication, updates, internal or external) is routed through the secure tunnel.

- This configuration is *not* compatible with the HTTP proxy configuration.
- SailPoint reserves the 172.16.0.0/22 IP range for secure tunnel communication. If any sources reside in this range, implementing this configuration will prevent those sources from properly routing traffic.
- SSH traffic cannot be routed publicly.
- This option makes it easy to generate a list of all outbound connections made by a VA during a specific window of time.
- This option allows customers to limit the various outbound connections generated by the VA.
- Deep-packet inspection is not supported.

Related Documentation: Configuration Guide for Virtual Appliances with Secure Tunnel

Network Requirements:

Port	Reason	Direction	IP Addresses	Description
22	SSH	Inbound	Internal Only (Recommended)	Only required if you want to SSH into or copy files onto the VA

443	HTTPS	Outbound	US: 52.206.133.183 52.206.132.240 52.206.130.59 Europe - Frankfurt: 35.157.132.22 35.157.185.79 35.157.251.228 Europe - London: 18.130.210.174 18.130.148.201 35.178.220.78 APAC - Sydney: 52.65.42.92 13.55.78.212 3.24.127.50	Used for secure tunnel initialization. All outbound HTTPS traffic will go through this port.

NOTE: Target systems might have their own port requirements. VAs must be allowed to communicate over the ports required by target systems.

VA Deployment Options

This section discusses strategies for deploying the VA, beyond the basics of selecting a local or cloud virtualization environment. We recommend you review all of the options presented to help inform your decisions about the strategy you ultimately choose to follow.

- Deploying VAs for High Availability and Disaster Recovery
  - Strategy 1 - All VAs Running
  - Strategy 2 - Switch Clusters
  - Strategy 3 - Standby Reactive Deployment
- VA Deployment in the DMZ

Deploying VAs for High Availability and Disaster Recovery

The need to factor High Availability (HA) and Disaster Recovery (DR) into your deployment decisions may be obvious, but it might help to also understand the following:

- Each source is associated with a specific VA cluster.
- Any actions performed on that source, such as aggregation, test connection, authentication, or provisioning are sent as requests to the VA cluster and form a queue.
- Each VA that's running continually polls the queue of requests sent to its associated VA cluster.

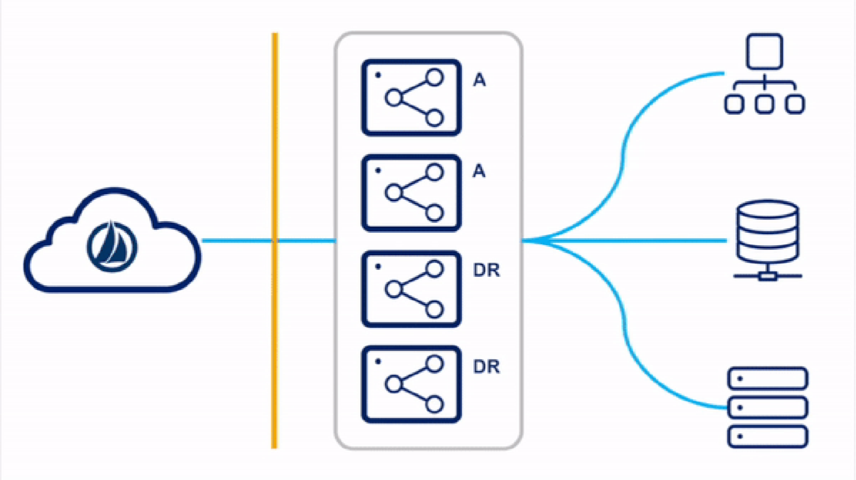
This section outlines different strategies for handling high availability and disaster recovery scenarios in virtual appliance deployments.

High Availability means ensuring that there are enough VAs running to meet the processing needs of the business, as well as sufficient redundancy to be able to compensate for a single VA becoming temporarily unavailable due to an upgrade process, loss of connectivity, or other activity that could otherwise result in downtime.

Disaster Recovery means making sure that your organization has VAs deployed in more than one location, as part of a failover strategy that ensures business continuity in the face of a disaster (natural or otherwise).

Strategy 1 - All VAs Running

In this strategy, all VAs are deployed in a single VA cluster, with all VAs running concurrently. Some VAs are in the primary datacenter, and others (called DR VAs) are deployed in a DR datacenter.



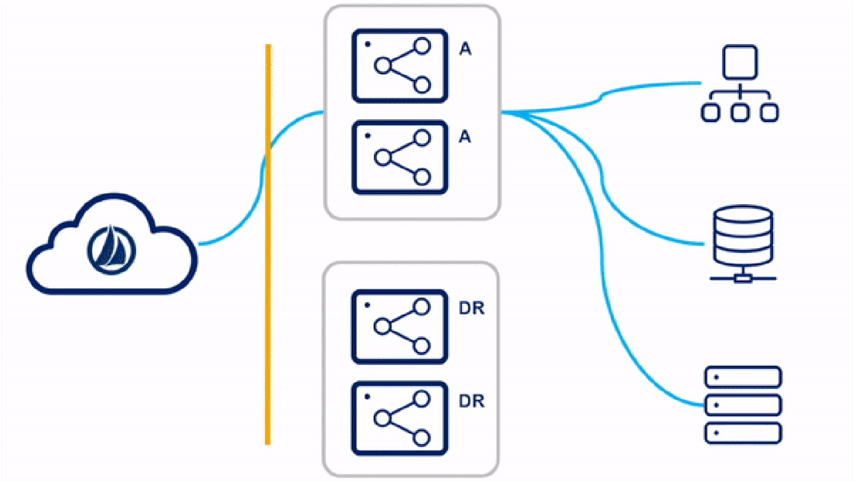
As work is assigned to the VA cluster, either primary VAs or DR VAs can pick up and perform requests. A problem could arise if there are latency issues between the source that the VA is communicating with and the VA's deployment location. This is especially true for DR VAs, which may be farther from the sources they are communicating with.

During a failover event, no action is needed. If the primary VAs go down, the DR VAs continue to respond to requests.

Advantages	**Disadvantages**
• On DR event, no action needed • Full utilization of all VAs • VAs stay up-to-date • Minimal risk of outages	• Potential latency issues

Strategy 2 - Switch Clusters

In this strategy, two VA clusters are deployed. One VA cluster is the 'primary VA cluster', with all member VAs in the primary datacenter. The other VA cluster is the 'DR VA cluster', with all member VAs in the backup DR datacenter. All VAs in all clusters are powered-on and receiving updates.



As work is assigned to the primary VA cluster, the primary VAs can pick up and fulfill requests. This mitigates any sort of latency issues between the source that the VA is communicating with and the VA deployment location. Even though the DR VAs are powered on, they are not receiving requests, because they are not associated with the primary VA cluster that the sources are using.

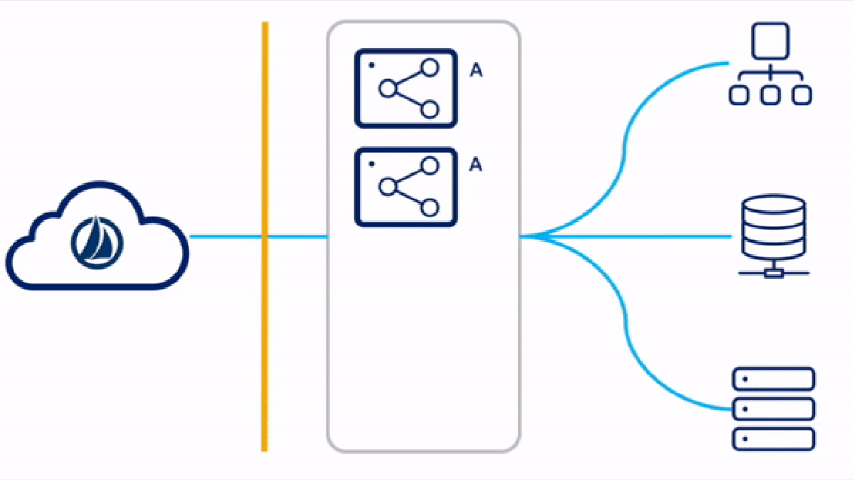
During a disaster event where the primary VAs go down, there would be an outage until the sources are reconfigured to use the DR VA cluster.

> **NOTE**: On failover, switching clusters requires reentering the source credentials. This can complicate the failover process if these credentials are not readily available to the administrator, or if there are many sources to manage.

Advantages	**Disadvantages**
• DR VAs stay up-to-date • DR VAs don't add latency, as they aren't processing anything until a DR event occurs	• No utilization of DR VA cluster • Reconfiguration needed upon DR event, involving reentering of source credentials • Difficult if large number of sources to manage

Strategy 3 - Standby Reactive Deployment

In this strategy, primary VAs are deployed in a single VA cluster. Only the VAs in the primary datacenter are running concurrently. There are existing standby VAs set up and tested in a DR zone, but not yet deployed to a VA cluster. These VAs can be left powered up or down.



As work is assigned to the primary VA cluster, the primary VAs can pick up and fulfill requests. This mitigates any sort of latency issues between the sources that the VA is communicating with and the VA deployment location.

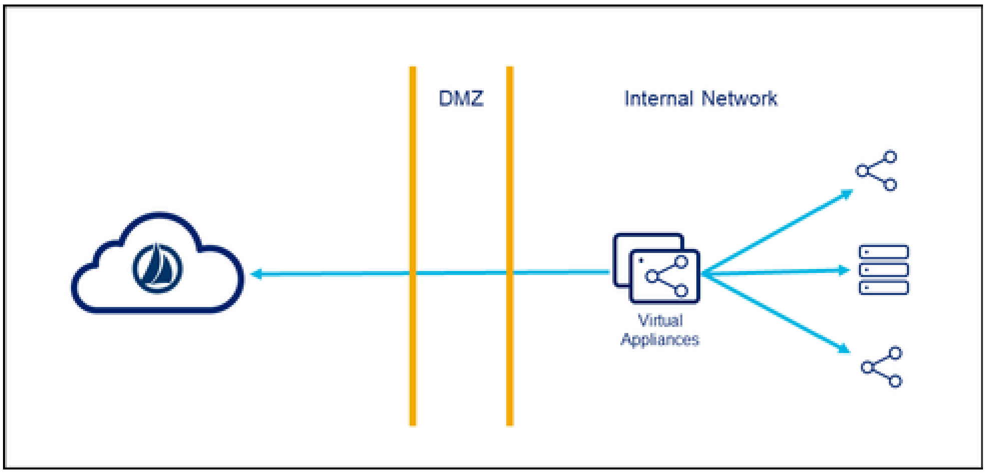
During a disaster event where the primary VAs go down, there would be an outage until the standby DR VAs are deployed to the primary VA cluster. As the new standby DR VAs come online, they start to fulfill requests.

> **NOTE**: We recommend you keep standby VAs tested and updated by frequently adding the VAs to an unused cluster dedicated for this purpose. After adding the standby VAs to this cluster, and allowing for some time to pass for updates to occur, the VAs can then be removed and powered down again.

Advantages	**Disadvantages**
• VAs don't add latency, as they aren't processing anything until a DR situation occurs	• Turnaround time can be greater depending on deployment of VA DR • Relies on VA readiness

VA Deployment in the DMZ

While there are no technical reason prohibiting it, we strongly recommend that you *not* deploy virtual appliances in the DMZ, or perimeter network. For the most secure and highest performing communication with target sources, we recommend that you deploy VAs near their sources on internal networks as shown in the following diagram.



Why Not Deploy in the DMZ?

We recommend against deploying the VA in the DMZ for the following reasons:

- **Security** - The most important consideration against DMZ deployment is security. A DMZ is a less-secure perimeter network by design. SailPoint VAs are hardened against attack, but they are a communication backbone with sources, and could be an attack vector. Each VA also contains the 2048-bit RSA asymmetric private key (generated from the chosen key passphrase), which is used to decrypt credentials when talking to various sources. Placing a VA in a less-secure zone could put your information at risk.

- **Proximity** - Virtual appliances connect to various sources, and both read (aggregation) and write (provisioning) activities can occur via API on these connections. Some connector APIs can be latency-sensitive. Deploying the VAs closer to the sources they are communicating with yields better performance.

- **Connectivity** - VAs are designed to communicate with internal sources, not perimeter sources. The purpose of a DMZ perimeter network is for externally-facing components to communicate with each other, not with components on the internal network. If a VA is deployed in the DMZ and needs to communicate with internal sources, you might have to open more ports on your internal firewall to facilitate that communication.

Best Practices Virtual Appliance (VA)

appliance
best connection coreos external outbound practices proxy secure tls
tunnel url va virtual whitelist
Add tags

👍 22 Kudos

Comment

Comments

esauve Mar 27, 2020 10

One remark regarding the whitelisted URLs. We discovered at our client that two additional URLs are needed to be whitelisted: ***coreos.com*** and ***fiji.identitynow.com***, where the latter one I'm not sure if that is region specific or not. Can these be added to the document?

kelly_wells Apr 23, 2020 10:

Thanks for the heads up, @esauve ! I've added both `*.coreos.com` and `*.identitynow.com` to the table to account for any variations of those domains.

SleepNoMore Feb 25, 2021 08

Hi!

I might've stumbled on an error in this documentation. I'm currently a part of an implementation where we've included the above-mentioned end-points in a FW whitelist. However, it seems as if there's an error in the recommended URL of amazonaws and coreos.

Documentation states that the following ought to be whitelisted:

```
*.coreos.com

*.core-os.net

*.s3.amazonaws.com

*.s3.us-east-1.amazonaws.com
```

However, upon doing troubleshooting on a virtual machine with these end-points specified in a FW whitelist, it returned:

```
\ns3.amazonaws.com => ERROR
\ncoreos.com => ERROR
\nsqs.us-east-1.amazonaws.com => ERROR
```

Removing *. from the whitelisted endpoints resolved the matter.

Hope this helps,
SleepNoMore

---

dirk_jahn Jul 09, 2021 04:

This guide states: "SailPoint reserves the 172.16.0.0/22 IP range" in the Secure Tunnel configuration option.

But the guide "Configuration Guide for Virtual Appliances with Secure Tunnel" states "We reserve the IP range 10.255.255.241/28"

Could somebody please validate and correct that ?

Thank you.

---

charles_chen Feb 03, 2022 06

Region-Specific AWS URLs table has three services - SQS, DynamoDB and Elastic Container Registry.

- sqs.us-east-1.amazonaws.com
- dynamodb.us-east-1.amazonaws.com
- 874540850173.dkr.ecr.us-east-1.amazonaws.com

  For APAC region-specific service URLs, assuming the following three:

  - sqs.ap-southeast-2.amazonaws.com
  - dynamodb.ap-southeast-2.amazonaws.com
  - 874540850173.dkr.ecr.ap-southeast-2.amazonaws.com is 874540850173 same for ap-southeast-2 region?

---

asedec001 Apr 14, 2022 12:1

We have lost our login details. Is there a way to reset it?

What is the default user name?

---

matt_herrera Apr 14, 2022 03:

@asedec001 You can contact support@sailpoint.com and they can assist.

Powered by Khoros