One Identity Safeguard for Privileged Sessions 6.7.2

Scalability and High Availability in Safeguard

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

SPS Scalability and High Availability in Safeguard
Updated - 24 November 2020, 08:54
Version - 6.7.2

Contents

Introduction

This document describes the different ways multiple appliances in the Safeguard product line can be deployed together.

Appliances of a Safeguard deployment: SPP and SPS

The Safeguard product line consists of two appliances: One Identity Safeguard for Privileged Passwords (SPP) and One Identity Safeguard for Privileged Sessions (SPS).

SPP appliances and SPS appliances provide different functionality. You can use them together or independently.

- SPP provides asset and account discovery, password rotation and management, and access request workflow.
- SPS provides transparent or non-transparent interception of remote admin protocols, audit recording and video-like playback of sessions and it runs One Identity Safeguard for Privileged Analytics (SPA) if it's licensed and enabled.

When used together, the two main operational modes are SPP-initiated (or Passwords-initated) and SPS-initiated (or Sessions-initiated).

- In SPP-initiated mode, users request access on the portal of SPP and when they are granted access, they are connected to the target account through SPS. For more information, see "Using SPS with SPP" in the Administration Guide.
- In SPS-initiated mode, users connect directly to a target server, SPS intercepts the traffic and fetches the required credentials from SPP.

SPP and SPS appliances solve scalability and high availability independently, but can interoperate to ensure the correct operation of the entire deployment.

Most important terms around clustering

Clustering

Clustering is a catch-all term that can often be used to mean different things. SPP and SPS appliances can be clustered to provide:

- Shared configuration
- Scalability
- High availability
- Disaster recovery
- Audit data replication
- Interoperation between SPP and SPS appliances

For clarity, try to use the term specific to the use case you want to discuss whenever possible.

High availability (HA)

Multiple SPP appliances and SPS appliances can be connected to ensure high availability. This enables the continuation of vital technology infrastructure and systems.

Disaster recovery (DR)

SPP appliances and SPS appliances can be connected to ensure immediate recovery following a natural or human-induced disaster. This technology reduces downtime and data loss.

Scalability

Another benefit of connecting multiple appliances is load distribution and scaling to loads beyond what a single appliance could serve, while still ensuring that the deployment can be configured and operated as a single solution instead of a bunch of independent appliances. Both SPP and SPS clustering provide scalability features to reduce management and operational costs.

SPP-SPS Join

An SPP cluster may be joined to one or more SPS clusters to combine their functionality, for example, to provide password rotation and session recording for the same accounts.

Overview of clustering in SPP and SPS

One Identity Safeguard for Privileged Passwords (SPP)

SPP ensures shared configuration, scalability, high availability, and disaster recovery through a single architecture. It is possible to join 3 or 5 SPP appliances into a single cluster. All important information is replicated along the entire cluster and the cluster remains functional if some appliances fail. Load can also be distributed amongst the appliances in the cluster.

One Identity Safeguard for Privileged Sessions (SPS)

SPS follows a different approach and solves high availability and disaster recovery independently of shared configuration and scalability.

- High availability can be ensured by adding a hot-spare pair to every SPS appliance that replicates all information from the first appliance and takes over all its functionality in case of a failure but serves no production traffic until the takeover occurs.
- Shared configuration and scalability are achievable by clustering multiple SPS appliances (or HA pairs of appliances) together to control and monitor them from a single pane of glass.

HA and scalability can be used at the same time but needs to be configured independently.

- An SPS HA pair always consists of exactly two nodes, a master and a minion.
- An SPS scalability cluster consists of an arbitrary number of nodes with varying roles that will be described in detail later.

SPP and SPS clusters can work together and support each other's HA and scalability models through the SPP-SPS join.

High Availability

The following describes how High Availability works in the Safeguard product line.

High Availability in One Identity Safeguard for Privileged Passwords (SPP)

In an SPP cluster, all vital data that is stored on the primary appliance is also stored on the replicas. The replicas provide a read-only view of the security policy configuration. You cannot add, delete, or modify the objects or security policy configuration on a replica appliance, but you can perform password change and check operations and make password release and session access requests. Users can log in to replicas to request access, generate reports, or audit the data. Also, passwords and sessions can be requested from any appliance in a Safeguard cluster.

In the event of a disaster, where the primary appliance is no longer functioning, you can promote a replica to be the new primary appliance.

The full operation requires that the cluster has consensus (quorum). Consensus means that a majority of the clustered appliances are online and able to communicate. If a cluster loses consensus, it goes into a read-only mode to prevent data inconsistencies and password check and change is disabled. You can configure whether you want to maintain or suspend access request workflows when consensus is lost via the Offline Workflow Mode setting.

For more information, see Disaster recovery and clusters in the One Identity Safeguard for Privileged Passwords Administration Guide.

High Availability in One Identity Safeguard for Privileged Sessions (SPS)

In case of physical appliances, high availability can be ensured by adding a hot-spare pair to every appliance. The two appliances are ideally placed adjacent to each other and are connected by a direct cross cable. The "minion" node in the pair replicates the entire disk contents of the "master" node, including all configuration and audit recordings. It keeps all of its outside network connections in a disconnected state and serves no traffic until it needs to take over the role of the master. Takeovers can be initiated manually, or they are performed automatically if the master node does not reply to the periodic heartbeat checks.

High availability is not available and not required for virtual appliances. The reason for that is that all enterprise virtualization environments support high availability on the hypervisor level, which will always be more optimal than what a host-based approach could provide.

For more information, see "Managing a High Availability One Identity Safeguard for Privileged Sessions (SPS) cluster" in the Administration Guide.

High Availability in joint SPP and SPS deployments

To provide high availability in joint deployments, have at least 3 SPP nodes and add high availability pairs to all SPS nodes. As described above, an SPP cluster of at least 3 nodes provides data redundancy and high availability for the SPP functionality. In case a hot-spare SPS appliance needs to take over the master role in an SPS HA pair, the SPP cluster will automatically direct new connections against the new master. This solves the availability of all audit information in case of a hardware failure, too.

Backups

Even though high availability protects against hardware failures, we always recommend enabling backups for both SPP and SPS appliances in both virtual and hardware deployments. It provides additional protection against:

- Software errors
- Mistakes made by the administrators
- Large-scale disasters that affect many nodes of a cluster at once

Backups, however, do not provide a sufficient level of high availability by themselves as data during backup periods can be lost and a full restore from a backup might lead to a long period of service outage.

For more information on configuring backups, see the respective sections in the Administration Guide:

- SPP: Backup and restore in the One Identity Safeguard for Privileged Passwords Administration Guide
- SPS: "Data and configuration backups" in the Administration Guide

Scalability

The following describes how scalability works in the Safeguard product line.

Scalability in One Identity Safeguard for Privileged Passwords (SPP)

The primary appliance in an SPP cluster automatically delegates platform management tasks (such as password check and password change) to appliances based on task load. By adding more appliances to the cluster, it becomes possible to perform more of these tasks.

It is possible to customize load balancing through the feature of Managed Networks. Managed networks are named lists of network segments serviced by a specific SPP appliance. Using managed networks, you can:

- Distribute the load so there is minimal cluster traffic.
- Use the appliances closest to the target asset to perform the actual task.

An SPP cluster has a default managed network that consists of all cluster members.

Password request workflows can be performed through any appliance in the cluster if the cluster is healthy. There's no automatic load balancing performed for those.

For more information on Managed Networks, see Managed Networks in the One Identity Safeguard for Privileged Passwords Administration Guide.

Scalability in One Identity Safeguard for Privileged Sessions (SPS)

Multiple SPS appliances or HA pairs of appliances can be joined into a cluster and managed from a single pane of glass.

Load balancing is not provided by the SPS cluster. It is up to the user to set network connections up in a way that distributes the load amongst them. If SPP and SPS are used together, SPP can be used to distribute the traffic, too (see the Joint SPP and SPS deployment section which follows).

It is possible to replicate the configuration of a master node amongst the entire cluster.

For more information, see "Managing a cluster with configuration synchronization without central search" in the Administration Guide.

It is also possible (but not mandatory) to make all audit information about the recorded sessions from all appliances available on a single search interface. This requires a dedicated search appliance (or HA pair).

For more information, see "Managing a cluster with central search configuration and configuration synchronization" in the Administration Guide.

Scalability in joint SPP and SPS deployments

In case of SPP-initiated workflows, it is possible to assign SPS scalability clusters to Managed Networks. The SPP cluster periodically checks the load on the members of the SPS cluster and assigns new connections to the best available appliance.

In case of SPS-initiated workflows, SPS appliances always target the primary appliance of the SPP cluster, but those queries don’t usually require scaling out to multiple SPP appliances.

Disaster Scenarios

The following describes how Disaster Scenarios work in the Safeguard product line.

Disaster Scenarios in One Identity Safeguard for Privileged Passwords (SPP)

Failure of a replica node

The cluster recognizes that this node is out of the circulation and automatically redirects traffic. All vital data is replicated between the nodes, so no data loss happens.

It is recommended that managed networks contain more than one appliance and if they do, other nodes will take over the tasks of the failed node. Managed networks can be reconfigured or disabled to provide continuity of service.

Failure of the primary node

Configuration changes are not possible, but normal operation continues. It is possible to change the primary manually to any of the replica nodes.

Failure of more than half of the cluster

The cluster switches into a read-only mode where config changes are not possible and password check and change tasks are paused. The Offline Workflow Mode setting can be used to manually or automatically restore access request workflow. If the majority of appliances have failed completely, a cluster reset operation can be used to change to a new primary without consensus. A backup restore is only necessary if all of the appliances in the cluster are lost.

Losing connectivity between appliances

The part of the cluster that gets isolated and sees less than half of the original cluster switches into read-only mode, whereas the bigger part remains active. Whether the isolated nodes continue serving access requests is configurable via the Offline Workflow Mode setting. When connection is re-established, the appliance state is automatically synchronized.

Disaster Scenarios in One Identity Safeguard for Privileged Sessions (SPS)

Failure of a node in an HA pair

If the failed node was the master, the hot-spare automatically takes over the IP address and all traffic. Ongoing connections are disconnected. No data is lost as everything is replicated between the pairs. After the failed node is replaced, a resync is required which might require up to 24 hours. In all failure scenarios below, if the failed node has an HA pair, it takes over all functionality automatically and the same recovery steps are required as listed above.

Failure of a managed node (non-master appliance) in the scalability cluster

If it did not have an HA pair, traffic going through that node will stop. It is up to the network configuration to handle the outage and redirect traffic to another appliance in the cluster. In case of SPP-initiated workflows, SPP will try to redirect the traffic towards a different SPS when the SPS configuration master becomes aware of the outage. If central search was enabled, it remains possible to perform searches but video-like playback of sessions won't be available.

Failure of the configuration master in a scalability cluster

If it did not have an HA pair, it won't be possible to make any configuration changes in the cluster, but functioning nodes will keep serving connections. It is not possible to move the config master role to a different appliance, it must be restored from a backup.

Failure of the search master in a scalability cluster

If it did not have an HA pair, it won't be possible to search in audit information but all other functionality will be unaffected. The other nodes will buffer audit information until the search master node becomes available again. They are able to survive ~24 hours of downtime when operating at full capacity. After that, they stop accepting new connections.

Losing connectivity between HA pairs

Both appliances check if they see the outside network and if they do (and it's only the other node that they've lost), both of them assume that they need to operate as master nodes. It will lead to a split-brain situation that will cause service outage and needs to be recovered manually. It is highly recommended to configure redundant HA links between the nodes.

For more information, see "Redundant heartbeat interfaces" in the Administration Guide.

Losing connectivity between nodes in a scalability cluster

Some functionality (like making config changes or searching in new audit information) will be lost until the outage is resolved, but individual nodes will continue serving new connections.

Disaster Scenarios in joint SPP and SPS deployments

The same scenarios are handled in the same way as they would be in case of individual SPP and SPS clusters. In addition to those, there are a few additional potential concerns:

SPP-initiated workflows

Losing the SPS config master

Losing the SPP primary appliance: everything works fine as long as configuration changes are not required, SPP nodes reach out to SPS directly.

SPS-initiated workflows

Losing the SPS config master

Losing the SPP primary appliance:

- SPS stores all the SPP cluster members and for password requests it connects to the first available node, starting with the primary. If that's not available, it will try other nodes.
- SPS fetches information about the SPP cluster from the IP address that it was joined with originally (the primary at the time of the join). If an SPP is available at that IP address (does not need to be the primary), the SPS cluster will learn about changes in the configuration.
- If the SPP cluster member can replaced/reconnected on the same address, no manual action needs to be taken and the traffic will not be interrupted.
- If a SPP cluster member is permanently lost and cannot be replaced/reconnected, the clusters need to be unjoined and rejoined using the new primary.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product