Skyhigh for Shadow IT Integration Prerequisites

This document lists the pre-requisites necessary for the deployment of Skyhigh for Shadow IT solution.

Please check the check box () against each item to indicate readiness of the specific pre-requisite.

Here is a checklist of items that are prerequisites for the commencement of the deployment:

1. Log sources: Identify the various log sources (Firewalls and Proxies) and provide a 1000 lines sample from all the distinct log sources. If the logs are being aggregated to a SIEM device, please provide sample that covers all distinct log feeds.

1. Enterprise Connector Machine:

Following are the minimum recommended specifications for the Enterprise Connector Virtual Machine-

|  |  |  |
| --- | --- | --- |
|  | Sandbox | Production |
| # of processing cores | 2 | 8 |
| RAM | 8 GB | 16 GB |
| HDD | 100 GB | 500 GB + 3 days of logs |
| Operating System | Windows Server 2016 and above, RedHat/CentOS 7 and above, 64-bit. | |

1. Network Connectivity:

Firewall rules for Skyhigh Enterprise Connector:

The Log Processor must be able to communicate with https://www.myshn.net and https://pstat.myshn.net over TCP 443. Please open firewall ports if needed from Enterprise Connector VM/Machine.

(Optional) In case of Custom Attributes, the following are the other pre-requisites to implement this integration:

Service user account on the Customer’s Active Directory Global Catalog with Read Only privileges.

LDAP Connectivity details to Customer’s Active Directory

List of AD attributes

Outgoing 389/TCP to LDAP Service

(Optional) In case of SIEM Integration, the following are the other pre-requisites to implement this integration:

Connectivity details of the SIEM Appliance.

Configure SIEM Appliance to accept logs from Skyhigh Enterprise Connector.

Appropriate Firewall rules to connect Skyhigh with SIEM appliance.

1. Accounts: The Log Processor will need administrator (or appropriate) access to install, execute and access your log files. The applications that will need access to the log files are the shnlps and shnlpcli executables.
2. Additional Features:

Guest IP tagging

Dashboard SSO

IP to username mapping

Custom Attributes

IaaS discovery

SIEM Integration

Closed loop remediation with McAfee, Bluecoat, and Panorama

These can be discussed with professional services resource during implementation.

Samples







