PacGenesis

Deployment Platform Guide

aspera
an IBM® company

Table of Contents:

About PacGenesis

From global organizations to media and entertainment companies, PacGenesis has over 10 years of experience in data security. We've partnered with the best providers of cybersecurity and high-speed file transfer solutions to enable business owners to scale their companies and keep data safe. We provide solutions to the everyday challenges organizations face, listening to pain points, auditing current technology, and suggesting and implementing solutions to fit those needs.

About IBM Aspera

IBM Aspera is the world's fastest file transfer system that allows companies to share large files or large volumes of files around the world instantly. Using its proprietary FASP® technology to deliver data at lightning-fast speed, businesses can migrate data, deliver data, automate workflows, collaborate, and sync data. IBM Aspera leverages blockchain technology to add an extra layer of security to your data as it moves through multi-cloud architectures.

PacGenesis Training Portal Information

PacGenesis provides clients with easy access to educational materials and services to help them on their journey to modernized, efficient data transfer. By creating an account for the PacGenesis training portal, clients and employees will have access to a library of educational training videos, easily downloadable assets for solution updates and features, and access to a mailing list to stay up-to-date on everything in the industry.

PacGenesis IBM Aspera Download Links & Documentation

After gaining access to the PacGenesis training portal, clients will have access to download links that help educate them on using IBM Aspera to maximize its capabilities. This includes documentation on the High Speed Transfer Server, Shares, Console, Proxy Gateway, and more directly from IBM Aspera. PacGenesis maintains a download portal to make sure that clients are provided with the latest versions.

For any questions or for a consultation on Professional Services to help design and build-out your secure and accelerated transfer environment, please reach out to PacGenesis at engineering@pacgenesis.com.

PacGenesis

HSTS Platform Guide

aspera
an IBM® company

Hardware

- **General Hardware for Standalone HSTS:**
    - Baremetal or Virtual Machine
    - Centos 7 or RHEL 7-8
    - 16+ cores
    - 32GB+ RAM
    - 10Gbps network connectivity
    - Storage
    - (Equivalent AWS if needed C5.9xlarge-c5.4xlarge)

- **Hardware based on Transfer Usage:**

MAX AGG THROUGH	SUPPORTABLE CONCURRENCY	NETWORK INTERFACE	PLATFORM	RAM	CPU	CORES
100 Mbps	10+	100 Mbps Strong Wifi	Laptop or PC with Win/Linux/Mac or Mobile Embedded Platform	2GB	1.7 GHZ x86	2 Core
500 Mbps	10+	1 GbE	Laptop or PC with Win/Linux/Mac or Entry Level Server	4GB	2.2 GHz x86	2-4 Core
1 Gbps	10+	1 GbE	Laptop or PC with Win/Linux/Mac Server	8GB	2.7 GHz x86	4 Core
2.5 Gbps	50+	10 GbE	Server Class with Linux or Windows	16GB	2.9 GHz x86	8 Core
5 Gbps	50+	10 GbE	Server Class with Linux	24GB	3.3 GHz x86	8 Core
7.5 Gbps	50+	10 GbE	High Perf Server Class with Linux	32GB	3.5 GHz x86	8 Core
10 Gbps	50+	10 GbE	High Perf Server Class with Linux	32GB	3.5 GHz x86	16 Core

Note: Chart provided as a general guideline and assumes that the Aspera software is the only application running on the computer during transfers. For example, Anti-Virus tools can negatively affect performance. Performance may also vary due to the user's computer, storage, network equipment manufacturer and IT infrastructure differences.

HSTS Firewall Requirements:

- **Inbound TCP/33001 (or other TCP port set for SSH connections):** The port for SSH connections.
  - Aspera recommends running the SSH server on non-default port (allowing inbound SSH connections on TCP/33001, and disabling inbound connections on TCP/22) to ensure that your server remains secure from SSH port scan attacks.

- **Inbound UDP/33001:** The port for FASP transfers, which use UDP/33001 by default, although the server may also choose to run FASP transfers on another port.

- **Inbound and outbound TCP/8080 and TCP 8443 (or other TCP ports set for HTTP/HTTPS fallback):** The ports for the HTTP fallback. If only HTTP or HTTPS is used, you need to open only that port. For more information on configuring HTTP fallback ports, see **Configuring HTTP and HTTPS Fallback.**

- **Local firewall:** If you have a local firewall on your server (like iptables), verify that it is not blocking your SSH and FASP transfer ports (such as TCP/UDP 33001).

Firewall Configuration for Entitlements:

Note: This is not needed if using a file license

If your transfer server operates with an entitlement and not a license, you must ensure that the Aspera License Entitlement Engine (ALEE) can communicate with the Aspera metering and billing system.

- Allow outbound traffic on TCP port 443.
- Ensure outbound access to api.ibmaspera.com

PacGenesis

Proxy Platform Guide

aspera
an IBM® company

Introduction

Including the suggested OS and Hardware for a standard deployment of IBM Aspera Proxy on a standalone server.

Hardware

- Standalone Proxy Server
- Baremetal or Virtual Machine
- Centos 7 or RHEL 7-8
- 8 cores
- 16GB+ RAM
- 1Gbps

Firewall

Allow appropriate FASP traffic (TCP/UDP 33001, UDP range for Windows HSTS), as well as receive HTTP/HTTPS requests on the Node API port (default TCP 9091/9092).

PacGenesis

Faspex Platform Guide

aspera
an IBM® company

Introduction

Suggested OS and Hardware for a standard deployment with Faspex and (HSTS) High Speed Transfer Server on their own standalone servers.

Hardware Standalone Faspex Server:

- Baremetal or Virtual Machine
- Centos 7 or RHEL 7-8
- 8 cores
- 16GB+ RAM
- 1Gbps
- (Equivalent AWS EC2 instance if needed c5.2xlarge)

Faspex Web Application Firewall Requirements:

- **Allow inbound TCP/80 and TCP/443:** The ports for end users to access the web app.
- **Allow TCP 9092** to the HSTS Transfer Node
- **Allow outbound SMTP traffic:** Faspex will be configured to send email notifications via customer-managed SMTP server. Allow outbound connectivity to SMTP server on appropriate port, typically tcp/25, tcp/465, or tcp/587.

PacGenesis

Shares Platform Guide

aspera
an IBM® company

Introduction

Complete steps for provisioning and deploying a fresh installation of the Shares Web Application. Including the suggested OS and Hardware for a standard deployment with Shares and (HSTS) High Speed Transfer Server on their own standalone servers. Using local storage and file license.

Hardware

- Standalone Shares Server
- Baremetal or Virtual Machine
- Centos 7 or RHEL 7-8
- 8 cores
- 16GB+ RAM
- 1Gbps
- (Equivalent AWS if needed c5.2xlarge)

Shares Firewall Requirements:

- **Allow inbound TCP/80 and TCP/443:** The ports for end users to access the web app.
- **Allow TCP 9092** to the HSTS Transfer Node
- **Allow outbound SMTP traffic:** Shares will be configured to send email notifications via customer-managed SMTP server. Allow outbound connectivity to SMTP server on appropriate port, typically tcp/25, tcp/465, or tcp/587.

PacGenesis

Console Platform Guide

aspera
an IBM® company

Introduction

Suggested OS and Hardware for a standard deployment of IBM Aspera Console web application. Using local storage and file license.

Server Hardware

- Standalone Console Server
- Baremetal or Virtual Machine
- Centos 7 or RHEL 7-8
- 8 cores
- 16GB+ RAM
- 1Gbps network connectivity
- Console Database Storage calculation -

Console generates data for every transfer session. Plan the size-growth of your database depending on the number of transfer sessions each day.

In terms of planning for the size growth of the database, the per-file records generate 1-2KB per file transfer, and the session records generate 8-12KB per session. For some size estimates, here are a few examples:

- 100 sessions per day of 1000 files each, all external transfers between managed and unmanaged nodes = approx 201 MB per day db growth, 6.03 GB per month, 73.4 GB per year.
- 1000 sessions per day of 1 file each, all internal between managed nodes = approx 28 MB per day, 840 MB per month, 10 GB per year.
- 1000 sessions per day, 10,000 files each, 50% internal between managed nodes, 50% external with unmanaged node = approx 30 GB per day, 900 GB per month, 11 TB per year.

Console Server Firewall Requirements:

- For the Web UI, allow inbound connections for HTTP or HTTPS Web access (for example, TCP/80, TCP/443).
- Allow outbound connections for SSH (to be used for Console to Administer HSTS Managed node) on a non-default, configurable TCP port (Suggested port TCP/33001).
- Allow an outbound connection for TCP/9092 to allow Console to connect with HSTS nodes for Node API calls.
- Console will be configured to send email notifications via customer-managed SMTP server. Allow outbound connectivity to SMTP server on appropriate port, typically tcp/25, tcp/465 or tcp/587.

HSTS Firewall Requirements for Console and transfer traffic:

- Allow Console an inbound connection on TCP 9092.
- To ensure that your server is secure, Aspera strongly recommends allowing inbound connections for SSH on TCP/33001 (or on another non-default, configurable TCP port), and disabling inbound connections on TCP/22.
- Allow inbound connections for FASP transfers (From Aspera Clients/Servers it will transfer with), which use UDP/33001 by default, although the server may also choose to run FASP transfers on another port. Note Windows nodes don't port shares so a range is needed. 1 port per concurrent transfer (Example for 20 concurrent 33001-33019)

Note: No servers are listening on UDP ports.
When an Aspera client initiates a transfer, the client opens an SSH session to the SSH server on the designated TCP port and negotiates the UDP port over which the data transfer will occur.

PacGenesis

Orchestrator Platform Guide

aspera
an IBM® company

Introduction

Including the suggested OS and Hardware for a standard deployment of IBM Aspera Orchestrator on a standalone server.

Hardware

- **General Hardware for Standalone HSTS:**
  - Baremetal or Virtual Machine
  - Centos 7 or RHEL 7-8
  - 16+ cores
  - 32GB+ RAM
  - 1Gbps network connectivity
  - (Equivalent AWS if needed c5.4xlarge)

Orchestrator Standalone Server Install and Configuration:

You will need to obtain the installer RPMs and a valid license key.

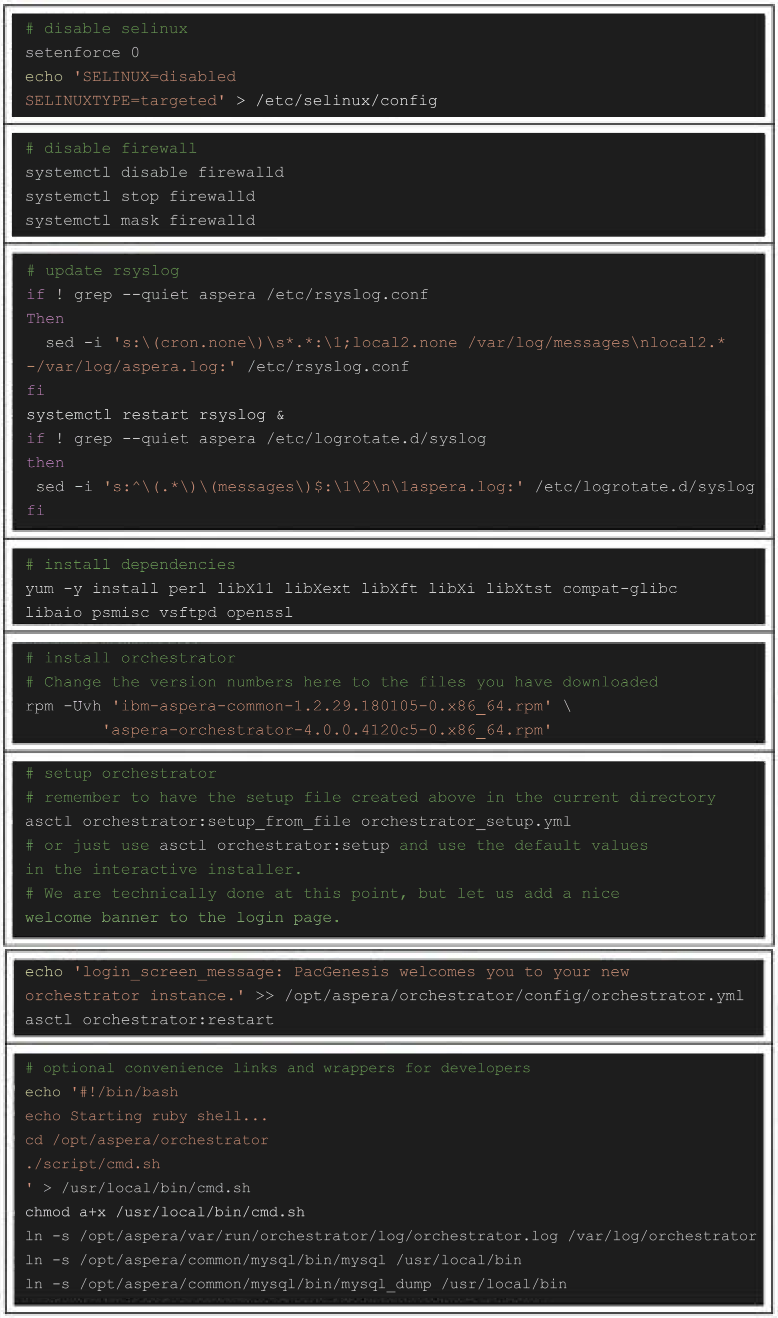
This example is installing these versions:

- Ibm-aspera-common-1.2.29.180105
- aspera-orchestrator-4.0.0.4120c5

This is also an example of a fully automated install.
Create a setup file named orchestrator_setup.yml with the following content:
The file includes responses to all questions normally asked by the installer.
You can skip this and just accept all defaults in the installer to get the same result.

```
---
:detailed: false
:uri_namespace: "/aspera/orchestrator"
:base_port: 3000
:mongrel_count: 3
:streamlined: true
:mysql_is_local: true
:setup_complete: false
:task_status: {}
:process_id:
:enabled: true
:ruby: 2.3.0
:force_new_branding: true
:database:
  :detailed: false
  :enabled: true
  :data_dir: "/opt/aspera/common/mysql/data"
  :port: 4406
  :user: root
  :hostname: 127.0.0.1
  :setup_complete: false
  :process_id:
  :password: aspera
  :allow_restart: true
:apache:
  :server_name: Apache HTTPD Server (Aspera)
  :admin_email: admin@orchestrator
  :http_port: 80
  :https_port: 443
  :balancer_port: 8080
  :log_level: error
  :httpd_account: ashttpd
  :httpd_group_account: ashttpd
  :use_ssl_chain_file: false
  :process_id:
  :setup_complete: false
  :detailed: false
  :ip: 0.0.0.0
  :ssl_enabled: true
  :ssl_cert: g
  :enabled: true
  :hostname: orchestrator
```

All commands in these console boxes are executed as root using bash as the shell. They can be copied and pasted directly into your terminal window. Some lines are broken into multiple lines in this document but will correctly copy and paste as a single line when required.



```
# disable selinux
setenforce 0
echo 'SELINUX=disabled
SELINUXTYPE=targeted' > /etc/selinux/config
```

```
# disable firewall
systemctl disable firewalld
systemctl stop firewalld
systemctl mask firewalld
```

```
# update rsyslog
if ! grep --quiet aspera /etc/rsyslog.conf
Then
  sed -i 's:\(cron.none\)\s*.*:\1;local2.none /var/log/messages\nlocal2.*
-/var/log/aspera.log:' /etc/rsyslog.conf
fi
systemctl restart rsyslog &
if ! grep --quiet aspera /etc/logrotate.d/syslog
then
 sed -i 's:^\(.*\)\(messages\)$:\1\2\n\1aspera.log:' /etc/logrotate.d/syslog
fi
```

```
# install dependencies
yum -y install perl libX11 libXext libXft libXi libXtst compat-glibc
libaio psmisc vsftpd openssl
```

```
# install orchestrator
# Change the version numbers here to the files you have downloaded
rpm -Uvh 'ibm-aspera-common-1.2.29.180105-0.x86_64.rpm' \
        'aspera-orchestrator-4.0.0.4120c5-0.x86_64.rpm'
```

```
# setup orchestrator
# remember to have the setup file created above in the current directory
asctl orchestrator:setup_from_file orchestrator_setup.yml
# or just use asctl orchestrator:setup and use the default values
in the interactive installer.
# We are technically done at this point, but let us add a nice
welcome banner to the login page.
```

```
echo 'login_screen_message: PacGenesis welcomes you to your new
orchestrator instance.' >> /opt/aspera/orchestrator/config/orchestrator.yml
asctl orchestrator:restart
```

```
# optional convenience links and wrappers for developers
echo '#!/bin/bash
echo Starting ruby shell...
cd /opt/aspera/orchestrator
./script/cmd.sh
' > /usr/local/bin/cmd.sh
chmod a+x /usr/local/bin/cmd.sh
ln -s /opt/aspera/var/run/orchestrator/log/orchestrator.log /var/log/orchestrator
ln -s /opt/aspera/common/mysql/bin/mysql /usr/local/bin
ln -s /opt/aspera/common/mysql/bin/mysql_dump /usr/local/bin
```

All that is required now is to login to the web interface of your new instance as user 'admin' with no password and upload your trial license key.