ANYWHERE Pre-Installation

Armor Knowledge Base

Topics Discussed

Resource Requirements

Requirement	Windows Instance	Linux Instance
CPU	2 Cores	1 Core
RAM	2GB	2GB
Disk Space	3GB	3GB
Bandwidth	Estimated 50-100Kb per minute, based on the logs generated in your system.	

Operating System Compatibility

Operating System	Supported Version for 64-bit Environments Only
CentOS	• 6.X • 7.X ⚠ To use a Linux-based Armor Anywhere agent, you must have Python 2.7 installed.
Red Hat Enterprise Linux (RHEL)	• 6.X • 7.X ⚠ To use a Linux-based Armor Anywhere agent, you must have Python 2.7 installed.
Ubuntu	• 16.04 • 18.04 ⚠ To use a Linux-based Armor Anywhere agent, you must have Python 2.7 installed.

Amazon Linux	• 2015.03 • 2015.09 • 2016.03 • 2016.09 • 2017.03 • 2017.09 • 2018.03 • Amazon Linux 2 ⚠ To use a Linux-based Armor Anywhere agent, you must have Python 2.7 installed.
Oracle Linux	• 6.X • 7.X ⚠ To use a Linux-based Armor Anywhere agent, you must have Python 2.7 installed.
Windows	• Microsoft Windows Server 2012 Standard • Microsoft Windows Server 2012 Datacenter • Microsoft Windows Server 2012 Enterprise • Microsoft Windows Server 2012 R2 Standard • Microsoft Windows Server 2012 R2 Datacenter • Microsoft Windows Server 2012 R2 Enterprise • Microsoft Windows Server 2012 R2 Foundation • Microsoft Windows Server 2016 Standard • Microsoft Windows Server 2016 Datacenter • Microsoft Windows Server 2016 Essentials • Microsoft Windows Server 2019 Standard • Microsoft Windows Server 2019 Datacenter • Microsoft Windows Server 2019 Enterprise ⚠ For Windows users, PowerShell 3 must be installed. ⚠ For Windows 2012 users, when you install the Armor Agent, the corresponding Trend Micro agent will require a reboot.

Browser Support

The Armor Management Portal (AMP) supports the current version of the following browsers:

- Chrome
- Firefox
- Internet Explorer
- Safari

⚠ Armor cannot guarantee that previous versions will be supported.

Firewall Rules

⚠ This topic only applies to **Armor Anywhere** users.

The following ports will need to be opened for each server registered with Armor Anywhere.

Inbound / Outbound	Service / Purpose	Port	Destination
Outbound	Armor Agent	443/tcp	• 146.88.106.210 • (api.armor.com)
Outbound	Malware Protection, FIM, IDS	• 4119/tcp • 4120/tcp • 4122/tcp	• 35.163.135.130 • 34.214.246.111 • 52.13.172.208 • (3a.epsec.armor.com)

Outbound	Log Management (Filebeat / Winlogbeat)	515/tcp	• 146.88.106.196
			  • (1a.log.armor.com)
			• 146.88.144.196
			  • (2a.log.armor.com)

Outbound	Monitoring	8443/tcp	• 146.88.106.200
			  • (1a.mon.armor.com)
			• 146.88.114.200
			  • (2a.mon.armor.com)

Outbound	Remote Access	443/tcp	• 146.88.106.216
			  • (1a.rs.armor.com)
			• 146.88.114.216
			  • (alternate)

Outbound	Vulnerability Scanning	*443/tcp	• 34.226.68.35
			• 54.144.111.231
			• 52.203.25.223
			• 34.236.161.191
			  • endpoint.ingress.rapid7.com
			  • (United States)
			
			• 52.60.40.157
			• 52.60.107.153
			  • ca.endpoint.ingress.rapid7.com
			  • (Canada)
			
			• 3.120.196.152
			• 3.120.221.108
			  • eu.endpoint.ingress.rapid7.com
			  • (Europe)
			
			• 52.64.24.140
			• 13.55.81.47
			• 13.236.168.124
			  • au.endpoint.ingress.rapid7.com
			  • (Australia)
			
			• 103.4.8.209
			• 18.182.167.99
			  • ap.endpoint.ingress.rapid7.com
			  • (Japan/Asia/Asia Pacific)

Inbound	Log Relay (Logstash)	• 5140/udp • 5141/tcp	The IP address for your virtual machine

Outbound	Log Relay (Armor's logging service (ELK))	• 5443/tcp • 5400-5600/tcp (Reserved) ⚠ Armor reserves the right to utilize this port range for future expansion or service changes.	1c.log.armor.com • These endpoints are served by the Amazon Elastic Load Balancers. As a result, the actual endpoints will vary dynamically across Amazon's IP ranges.

⚠ The agent will perform a lookup to the applicable DNS entry, which may resolve to one of multiple Amazon Web Services based subnets. As a result, if your firewall does not support outbound filtering by domain name, then you may need to open all outbound traffic to 443/tcp to accommodate this service.

⚠ Additionally, verify that your proxy server can externally communicate.

⚠ If your network environment's servers are behind specific firewall controls that block regular outbound communication, then you may want to perform a port-forwarding server deployment. To learn more, see Port-Forwarding and Proxy Server and Client Deployment.

After you install the agent, Armor recommends that you test the connection for each configured firewall rule.

To verify connectivity to an Armor service endpoint, use the telnet command.

The following example tests connectivity to api.armor.com over 443/tcp:

```
telnet 75.2.84.73 443
```

For Windows systems without the telnet feature installed, you can also use PowerShell:

```
new-object System.Net.Sockets.TcpClient('75.2.84.73', 443)
```

Remove Anti-Virus Software

Before you install the Armor Anywhere agent, you must remove any previously installed anti-virus software, such as Trend Micro, McAfee, etc. Afterwards, you must reboot your system.

Pre-Installation Scripts

Before you install the Anywhere agent, you can run the following scrips to verify that your environment is compatible.

Operating system	Script

• **Linux**
  • CentOS
  • Red Hat Enterprise Linux
  • Ubuntu
  • Amazon Linux
  • Oracle
	`sudo curl -sSL https://get.core.armor.com/latest/armor_agent.sh | sudo bash /dev/stdin`

• **Windows 2012** • **Windows 2016**	`[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest https://get.core.armor.com/latest/armor_agent.ps1 -outfile armor_agent.ps1 ; .\armor_agent.ps1`

Related Documentation

- ANYWHERE Installation
- Port-Forwarding and Proxy Server and Client Deployment