

Installation and Configuration Guide

ArcSight Express 4.0 Virtual Appliance

March 31, 2014



Copyright © 2014 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI .
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
03/31/2014	1.0	First release of guide and virtual appliance

Contents

Chapter 1: Overview 5

Chapter 2: Installing the ArcSight Express Virtual Appliance 7

 Supported ESXi Version and Required Hardware 7

 Operating System 7

 FIPS Support 8

 Browser Support 9

 Downloading the ArcSight Express Virtual Appliance OVA Files 9

 Upgrade Support 9

 Deploying the ArcSight Express Virtual Appliance OVA File 9

 Installing a License File 13

Chapter 1

Overview

The ArcSight Express Virtual Appliance is a Security Information and Event Management (SIEM) solution that collects and analyzes security data from heterogeneous devices on your network and provides you a central, real-time view of the security status of all devices that are of interest to you.

ArcSight Express components gather and store events generated by the devices you identify. These events are filtered and correlated with events from other devices or collection points to discover risks and assess vulnerabilities.

ArcSight Express uses the Correlation Optimized Retention and Retrieval Engine Storage (CORR-Engine Storage), a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches. This provides a number of benefits, including increased performance and more compact data storage.

The ArcSight Express Virtual Appliance allows deployment of ArcSight Express on servers that have VMware ESXi installed.

Installing the ArcSight Express Virtual Appliance

The following topics are covered in this chapter:

- ["Supported ESXi Version and Required Hardware" on page 7](#)
- ["Operating System" on page 7](#)
- ["Browser Support" on page 9](#)
- ["Downloading the ArcSight Express Virtual Appliance OVA Files" on page 9](#)
- ["Deploying the ArcSight Express Virtual Appliance OVA File" on page 9](#)
- ["Installing a License File" on page 13](#)

Supported ESXi Version and Required Hardware

The ArcSight Express Virtual Appliance is supported on VMware ESXi 5.5. The hardware requirements for installing the ArcSight Express Virtual Appliance OVA file are:

- 12 CPU cores
- 36 GB of RAM
- 1.8 TB disk available

Operating System

The ArcSight Express Virtual Appliance operating system is Centos 6.2 and the following security patches:

- bind-libs-9.8.2-0.17.rc1.el6_4.4.x86_64.rpm
- bind-utils-9.8.2-0.17.rc1.el6_4.4.x86_64.rpm
- cups-1.4.2-50.el6_4.4.x86_64.rpm
- cups-libs-1.4.2-50.el6_4.4.x86_64.rpm
- cvs-1.11.23-15.el6.x86_64.rpm
- dbus-glib-0.86-6.el6.x86_64.rpm
- dhclient-4.1.1-34.P1.el6.centos.x86_64.rpm
- dhcp-common-4.1.1-34.P1.el6.centos.x86_64.rpm
- freetype-2.3.11-14.el6_3.1.x86_64.rpm
- ghostscript-8.70-15.el6_4.1.x86_64.rpm

- krb5-appl-clients-1.0.1-7.el6_2.1.x86_64.rpm
- krb5-libs-1.10.3-10.el6_4.2.x86_64.rpm
- krb5-workstation-1.10.3-10.el6_4.2.x86_64.rpm
- liberation-fonts-common-1.05.1.20090721-5.el6.noarch.rpm
- liberation-sans-fonts-1.05.1.20090721-5.el6.noarch.rpm
- libexif-0.6.21-5.el6_3.x86_64.rpm
- libjpeg-turbo-1.2.1-1.el6.x86_64.rpm
- libpng-1.2.49-1.el6_2.x86_64.rpm
- libproxy-0.3.0-4.el6_3.x86_64.rpm
- libproxy-bin-0.3.0-4.el6_3.x86_64.rpm
- libproxy-python-0.3.0-4.el6_3.x86_64.rpm
- libsmbclient-3.6.9-151.el6.x86_64.rpm
- libtalloc-2.0.7-2.el6.x86_64.rpm
- libtdb-1.2.10-1.el6.x86_64.rpm
- libtiff-3.9.4-9.el6_3.x86_64.rpm
- libvorbis-1.2.3-4.el6_2.1.x86_64.rpm
- libxml2-2.7.6-12.el6_4.1.x86_64.rpm
- libxml2-python-2.7.6-12.el6_4.1.x86_64.rpm
- nspr-4.9.2-1.el6.x86_64.rpm
- nss-3.14.0.0-12.el6.x86_64.rpm
- nss-sysinit-3.14.0.0-12.el6.x86_64.rpm
- nss-util-3.14.0.0-2.el6.x86_64.rpm
- openjpeg-libs-1.3-9.el6_3.x86_64.rpm
- openssl-1.0.0-27.el6_4.2.x86_64.rpm
- perl-5.10.1-131.el6_4.x86_64.rpm
- perl-libs-5.10.1-131.el6_4.x86_64.rpm
- perl-Module-Pluggable-3.90-131.el6_4.x86_64.rpm
- perl-Pod-Escapes-1.04-131.el6_4.x86_64.rpm
- perl-Pod-Simple-3.13-131.el6_4.x86_64.rpm
- perl-version-0.77-131.el6_4.x86_64.rpm
- pixman-0.26.2-5.el6_4.x86_64.rpm
- samba-client-3.6.9-151.el6.x86_64.rpm
- samba-common-3.6.9-151.el6.x86_64.rpm
- samba-winbind-3.6.9-151.el6.x86_64.rpm
- samba-winbind-clients-3.6.9-151.el6.x86_64.rpm
- sudo-1.8.6p3-7.el6.x86_64.rpm
- xulrunner-17.0.6-2.el6.centos.x86_64.rpm
- yelp-2.28.1-17.el6_3.x86_64.rpm

FIPS Support

FIPS is not supported for this release of the virtual appliance.

Browser Support

Supported browsers for connecting to the ESM Manager are:

- Internet Explorer 9 and 10
- Firefox 24

Downloading the ArcSight Express Virtual Appliance OVA Files

The ArcSight Express Virtual Appliance OVA files are available for download from the HP Software Depot at:

<http://software.hp.com>.

If you use Internet Explorer to download the files, ensure that the files names remain as shown below.

Download the 3 files and the MD5 checksum to a disk accessible by your vSphere client:

- B7500_B1312_1800GB_V8.ova.part1
- B7500_B1312_1800GB_V8.ova.part2
- B7500_B1312_1800GB_V8.ova.part3

Join the 3 files into one file by running one of the following commands:

Windows - copy /b

```
B7500_B1312_1800GB_V8.ova.part1+B7500_B1312_1800GB_V8.ova.part2+B7500_B1312_1800GB_V8.ova.part3 B7500_B1312_1800GB_V8.ova
```

Linux - cat B7500*.part* > B7500_B1312_1800GB_V8.ova

After joining the 3 files together, use the MD5 checksum to verify the file's integrity.

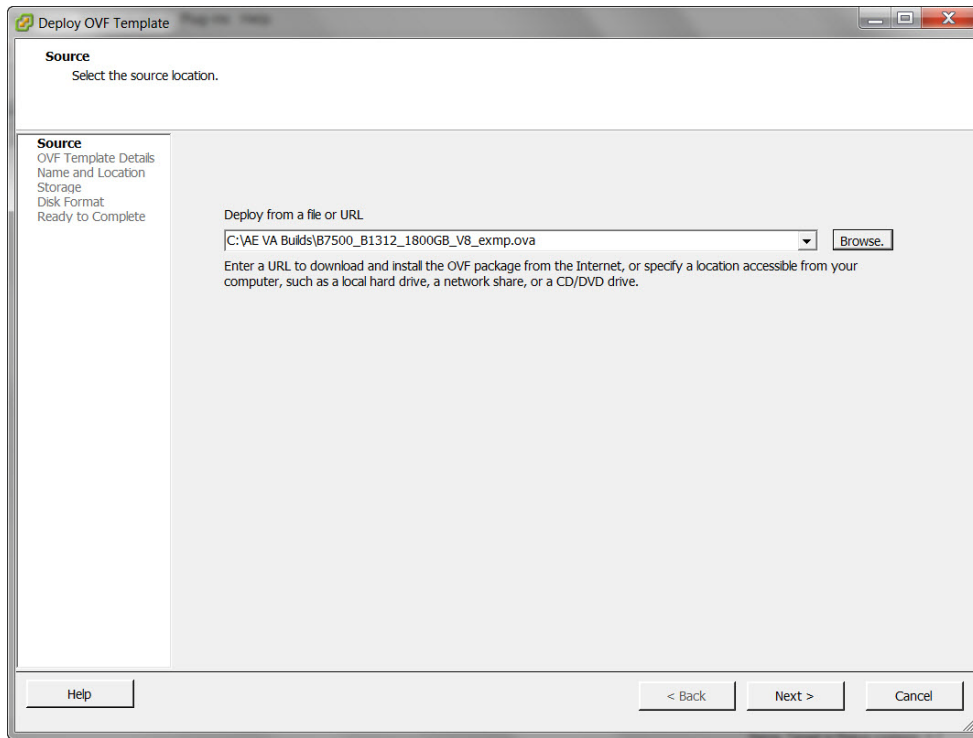
Upgrade Support

The ArcSight Express 4.0 Virtual Appliance cannot be upgraded from any prior versions of ArcSight Express.

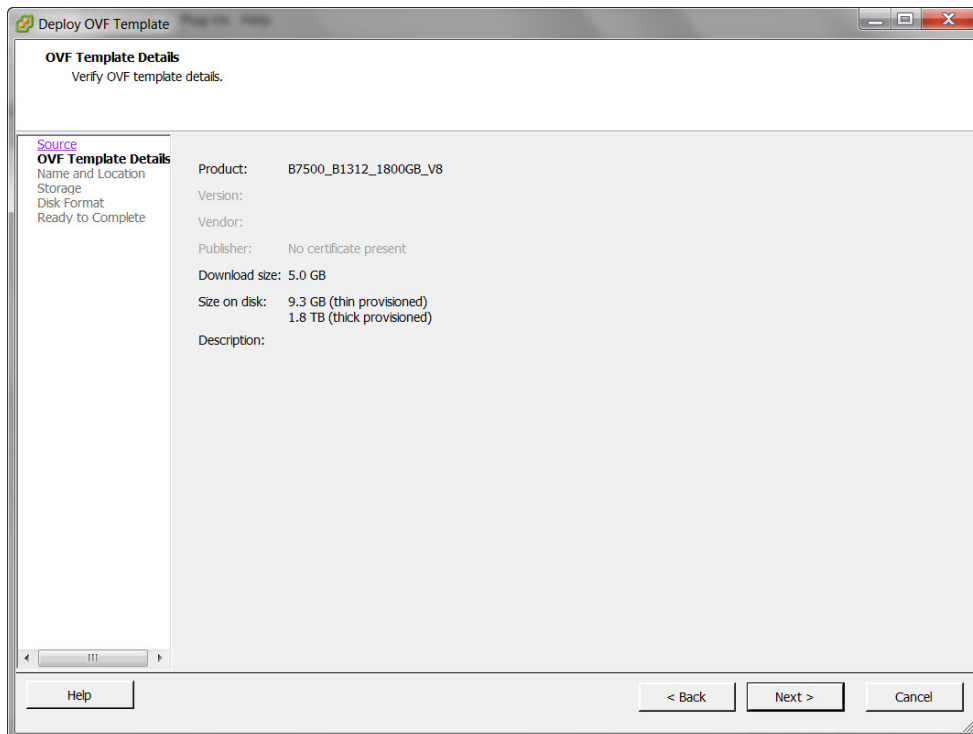
Deploying the ArcSight Express Virtual Appliance OVA File

To deploy the virtual appliance OVA file, use a vSphere client to perform the following procedure:

- 1 Select **File > Deploy OVF Template**. The Source screen displays:



- 2 Click **Browse** and navigate to where you downloaded the OVA file.
- 3 Select the file and then click **Next**. The OVF Template Details screen displays:



- 4 Click **Next**. The Name and Location screen displays:

Deploy OVF Template

Name and Location
Specify a name and location for the deployed template

Source
OVF Template Details
Name and Location
Storage
Disk Format
Ready to Complete

Name:
B7500_B1312_1800GB_exmp
The name can contain up to 80 characters and it must be unique within the inventory folder.

Help < Back Next > Cancel

- 5 Enter a name for the virtual appliance or accept the default. You can change the name later. Click **Next**. The Storage screen displays:

Deploy OVF Template

Storage
Where do you want to store the virtual machine files?

Source
OVF Template Details
Name and Location
Storage
Disk Format
Ready to Complete

Select a destination storane for the virtual machine files:

Name	Drive Ty...	Capacity	Provisio...	Free	Type	Thin Provision..	Access
n15-214-1...	SSD	737.50 GB	975.00...	736.55	VMFS5	Supported	Single ho...
n15-214-1...	Non-SSD	8.73 TB	3.56 TB	5.18 TB	VMFS5	Supported	Single ho...

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Ty...	Capacity	Provisioned	Free	Type	Thin Provisioning	Access
------	-------------	----------	-------------	------	------	-------------------	--------

Compatibility:

Help < Back Next > Cancel

- 6 Select a drive with 1.8 TB of disk space. The virtual appliance requires 1.8 TB of disk space. Click **Next**. The Disk Format screen displays:

The screenshot shows the 'Disk Format' screen of the 'Deploy OVF Template' wizard. The title bar reads 'Deploy OVF Template'. The main heading is 'Disk Format' with the subtext 'In which format do you want to store the virtual disks?'. On the left, a navigation pane lists 'Source', 'OVF Template Details', 'Name and Location', 'Storage', 'Disk Format' (which is highlighted), and 'Ready to Complete'. The main area contains a 'Datastore:' field with the value 'n15-214-133-h86_dat' and an 'Available space (GB):' field with the value '5304.9'. Below these are three radio button options: 'Thick Provision Lazy Zeroed' (which is selected), 'Thick Provision Eager Zeroed', and 'Thin Provision'. At the bottom, there are three buttons: 'Help', '< Back', and 'Next >', along with a 'Cancel' button.

- 7 Select the **Thick Provisioned Lazy Zeroed Format**. Click **Next**. The Ready to Complete screen displays.

The screenshot shows the 'Ready to Complete' screen of the 'Deploy OVF Template' wizard. The title bar reads 'Deploy OVF Template'. The main heading is 'Ready to Complete' with the subtext 'Are these the options you want to use?'. On the left, the same navigation pane as in the previous screen is shown, with 'Ready to Complete' highlighted. The main area contains the text 'When you click Finish, the deployment task will be started.' followed by a section titled 'Deployment settings:' which lists the following details: 'OVF file: C:\AE VA Builds\B7500_B1312_1800GB_V8_exmp.ova', 'Download size: 5.0 GB', 'Size on disk: 1.8 TB', 'Name: B7500_B1312_1800GB_exmp', 'Host/Cluster: n15-214-133-h86.arst.usa.hp.com', 'Datastore: n15-214-133-h86_datastore2', 'Disk provisioning: Thick Provision Lazy Zeroed', and 'Network Mapping: "VM Network" to "VM Network"'. At the bottom, there is a checkbox labeled 'Power on after deployment' which is currently unchecked. The bottom buttons are 'Help', '< Back', 'Finish', and 'Cancel'.

- 8 If the deployment settings are correct, click **Finish**. A progress timer will appear showing the progress of the deployment. When the deployment completes, the virtual machine created from the OVA file is added to the inventory (Virtual Machines tab) on your vSphere client.
- 9 Right-click your VM and select **Power > Power Off**.
- 10 Before running the First Boot Wizard, configure your network settings and increase the memory from 12 GB to 36 GB. To configure the network settings and increase the memory for your virtual appliance, right-click your virtual machine in the Virtual Machines tab. Select **Edit Settings**.

After configuring the network settings and increasing the memory for your virtual machine, select **Power > Power On**. The virtual machine performs an initial boot process that displays in the console. After installing the license, refer to the Configuring the ArcSight Express chapter of the ArcSight Express with CORR-Engine 4.0 Configuration Guide. The guide is available at:

<https://protect724.arcsight.com>

Installing a License File

The ArcSight Express Virtual Appliance requires that a license be installed.

Perform the following procedure to install the license:

- 1 Download the license file from the Customer Support web site at <http://support.openview.hp.com> to a computer from which you can connect to the virtual appliance.
- 2 Follow the **First Boot Wizard** directions for license installation.
- 3 Click **Browse** and navigate to where you stored the license and select the license file.
- 4 Click **Upload & Install**.
- 5 Perform the rest of the First Boot Wizard steps.

The base license includes:

- 4 onboard connectors
- 25 remote connectors
- 3 console users
- 25 web users
- 2500 IDView users
- 1500 devices
- 25000 assets
- Threat detector enabled

The base license includes 250 sustained events-per-second (EPS). Additional EPS can be added only in increments of 250 up to a maximum of 1250.

Pattern Discovery jobs can be resource intensive. Under high EPS, Pattern Discovery jobs can cause a degradation in performance, and may fail to return a matching result set. ArcSight recommends that you reduce the number of events over which the Pattern Discovery search runs and/or frequency of Pattern Discovery jobs when running a system with high EPS.

