Installation, Configuration, and Upgrade Guide (Currently in Progress--DRAFT)

HawkEye AP 6.2.0
May 4, 2016

Hexis Cyber Solutions, Inc.
2800 Campus Drive, Suite 150
San Mateo, CA 94403
+1 855 529-3929
www.hexiscyber.com

Copyright

Trademarks

The Hexis Cyber Solutions® logo and HawkEye AP are registered trademarks of Hexis Cyber Solutions, Inc., in the United States. Other company, product names or logos mentioned or reproduced in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Patents

The software described in this manual contains technology protected by U.S. Patent 7,024,414.

Permitted Use

This document is provided by Hexis Cyber Solutions, Inc., and/or its subsidiaries to entities using the services described herein pursuant to a separate services and/or software license agreement. This document may be used by such entities only for the limited purpose of using the services described herein as authorized by such services agreement. Any other use of this document is strictly prohibited, unless expressly authorized by Hexis Cyber Solutions, Inc., in writing.

Disclaimer and Limitation of Liability

Except as otherwise expressly provided in the applicable services and/or software license agreement, Hexis Cyber Solutions, Inc., and its subsidiaries make no representations or warranties of any kind, whether express or implied, regarding the accuracy of this document and disclaim the implied warranties of merchantability, fitness for a particular purpose, title and non-infringement of third party rights, to the maximum extent permitted by law. Hexis Cyber Solutions, Inc., and its subsidiaries assume no responsibility for any damage or loss resulting from the use of this document. This document is subject to revision from time to time.

Confidential Information

The information contained in this document is confidential and proprietary to Hexis Cyber Solutions, Inc., and its subsidiaries and may not be used or disclosed except as expressly authorized in writing by Hexis Cyber Solutions, Inc. This document is released to the possessor on a strictly secure basis. No authority, express or implied, exists to permit discussion with any third party. By continuing to possess this document, the bearer accepts all direct and indirect responsibility for keeping these materials in confidence. The bearer acknowledges the implicit material commercial harm to Hexis Cyber Solutions, Inc., of unauthorized disclosure of the contents herein, including an acknowledgment of responsibility for such damages caused to Hexis Cyber Solutions, Inc., if any.

Destination Control Statement

ECCN (Export Control Classification Number):5D002 ENC

These commodities, technology, or software were exported from the United States in accordance with the Export Administration Regulations. Diversion contrary to United States law is prohibited.

TABLE OF CONTENTS

Preface

This book, the *Installation, Configuration, and Upgrade Guide*, describes the 6.2.0 version of HawkEye AP. It documents the procedures for downloading, installing, configuring, and upgrading the HawkEye Event Data Warehouse (EDW) and the Collector, Analyzer, and Analytics, and other related components.

This Preface contains the following sections:

- "Audience for this Book", next
- "Installation, Configuration, and Upgrade Guide Organization", on page 7
- "Road Map to HawkEye AP Documentation", on page 8
- "Conventions Used in HawkEye AP Documentation", on page 9
- "Contacting Technical Support", on page 11

Audience for this Book

This book is directed to system administrators who install and manage software systems.

Installation, Configuration, and Upgrade Guide Organization

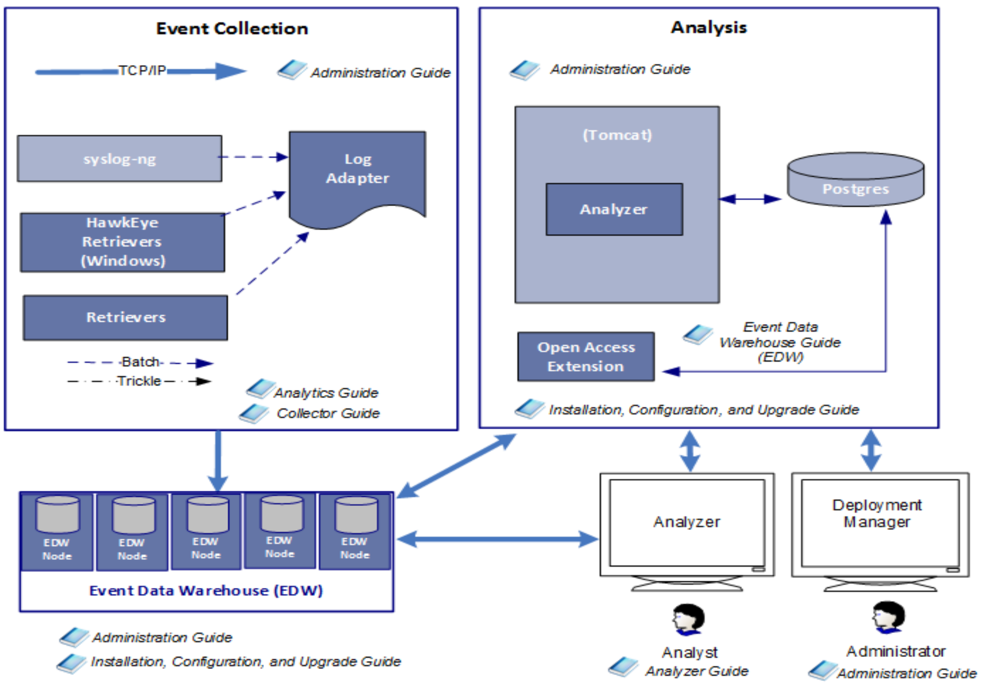
This book contains the following chapters:

- Chapter 1: HawkEye AP Overview—Identifies HawkEye AP components and how they work together to deliver the HawkEye AP Solution. Included is an introduction to HawkEye AP concepts and deployment configuration options for installation.
- Chapter 2: Preparing to Install HawkEye AP—Describes pre-installation tasks required to install HawkEye AP.
- Chapter 3: Installing and Configuring HawkEye AP—Provides step-by-step instructions to install and configure HawkEye AP using the Cluster Wizard.
- Chapter 4: Extending the Event Data Warehouse (EDW)—Provides step-by-step instructions to extend the Event Data Warehouse.
- Chapter 5: Upgrading from HawkEye AP 6.0.1 to 6.1.0—Provides step-by-step instructions to upgrade HawkEye AP using the Cluster Wizard.
- Chapter 6: Upgrading from HawkEye AP 5.0.1 to 6.2.0—Provides step-by-step instructions to upgrade HawkEye AP using the Cluster Wizard.
- Chapter 7: Removing Your Deployment of HawkEye AP Software—Provides instructions to remove deployment. of the HawkEye AP software.
- Chapter A: Installer Data Collection Checklist—Presents a checklist of information that you are required to provide the HawkEye AP during installation.

Road Map to HawkEye AP Documentation

This document, the *Installation, Configuration, and Upgrade Guide*, is part of the larger documentation set of your HawkEye AP system. Figure P-1 illustrates HawkEye AP components and modules in the context of their function within the HawkEye AP system.

Figure P-1: Road Map to HawkEye AP Documentation



The table below describes all the manuals in the HawkEye AP documentation set and the user roles to which they are directed.

Role	Tasks	Documentation
Analyst, Report Developer, System Administrator	• Create and edit reports, charts, and models • Create and edit dashboards • Manage HawkEye AP Users • Manage HawkEye AP Models • Create and edit data models • Write SQL code and queries	*Analyzer Guide*
Business Analyst or System Administrator	• Learn about Analytics • Use IntelliSchema views • Learn about the Foundation and Compliance Analytics packages • Learn about additional Analytics packages	*Analytics Guide*

Role	Tasks	Documentation
Developer, Report Developer or Security Analyst	• Use HawkEye AP SQL, HawkEye AP SQL functions, and libraries to create reports or query the EDW • Access EDW data using open standards as ANSI SQL, ODBC, and JDBC • Create and use Perl code in HawkEye AP SQL statements • Use the DBD Driver to query HawkEye AP from other locations	*Event Data Warehouse Guide*
Security System Administrator	• Configure retrievers, receivers, and collectors • Enable/disable log adapters • Configure HawkEye Retriever • Create log adapter PTL files	*Collector Guide*
System Administrator	• Install HawkEye AP • Configure HawkEye AP and its components • Configure Vmware	*Installation, Configuration, and Upgrade Guide*
System Administrator	• Manage the HawkEye Event Data Warehouse (EDW) • Manage the Collector • Manage users, groups, and permissions • Archive to nearline storage • Manage assets & monitor security alerts • Monitor log source health • Monitor system health • Troubleshoot • Error Messages	*Administration Guide*
Legal	Monitor third-party licenses	*Third-Party Open Source Licensing*

TIP: You can access the manuals listed above from:

- HawkEye AP Welcome page

  Click the **Documentation** hyperlink.

CONVENTIONS USED IN HAWKEYE AP DOCUMENTATION

This convention...	Indicates...	Example
bold text	Names of user interface items, such as field names, buttons, menu choices, and keystrokes	Click **Clear Filter**.
italic text	Indicates a variable name or a new term the first time it appears	`http://`*`<host>`*`:`*`<port>`*`/index.mhtml`

<table>
<tr><th>This convention...</th><th>Indicates...</th><th>Example</th></tr>
<tr><td>Courier text</td><td>Indicates a literal value, such as a command name, file name, information typed by the user, or information displayed by the system</td><td>atquery localhost:8072 myquery.sql</td></tr>
<tr><td>Small Caps</td><td>Indicates a key on the computer keyboard</td><td>Press Enter.</td></tr>
<tr><td>{ }</td><td>In a syntax line, curly braces surround a set of options from which you must choose one and only one.
NOTE: Syntax specifications for SELECT statements include curly braces as part of the {INCLUDE_BAD_LOADS] keyword.</td><td>{ start | stop | restart }</td></tr>
<tr><td>[ ]</td><td>In a syntax line, square brackets surround an optional parameter</td><td>atquery [options] <*host*>:<*port*> -</td></tr>
<tr><td>|</td><td>In a syntax line, a pipe within square brackets or curly braces separates a choice between mutually exclusive parameters
NOTE: Syntax for defining a Nearline Storage Address (NSA) includes a pipe.</td><td>{ start | stop | restart }
[g|m]</td></tr>
<tr><td>...</td><td>In a syntax line, ellipses indicate a repetition of the previous parameter</td><td>The following example indicates you can enter multiple, comma-separated options: <*option*>[, <*option*>[…]]</td></tr>
<tr><td>backslash (\)</td><td>A backslash in command-line syntax or in a command example behaves as the escape character on Unix. It removes any special meaning from the character immediately following it. In HawkEye AP documentation, a backslash nullifies the special meaning of the newline character as a command terminator. Without the backslash, pressing Enter at the end of the line causes the Unix system to execute the text preceding the Enter. Without the backslash, you must allow long commands to wrap over multiple lines as a single line.</td><td>atquery --user=administrator \
--pass=pass:p@ss localhost:8072\
-e='SELECT * FROM system.users;'</td></tr>
</table>

CONTACTING TECHNICAL SUPPORT

For additional help, email support@hexiscyber.com or call +1 855 529-3929. Also see the Hexis Cyber Solutions Technical Support web page at http://www.hexiscyber.com/content/ for HawkEye AP documentation, product downloads, and additional information on contacting support to escalate help on issues that impact your production environment.

CHAPTER 1

HawkEye AP Overview

This chapter introduces you to the HawkEye AP components that you will be installing. It contains an overview of HawkEye AP concepts and processes that are used to deliver the HawkEye AP solution. Included also is a discussion of basic HawkEye AP architecture options to plan your own HawkEye AP configuration and deployment.

The HawkEye AP Solution

This section describes the following topics:

- “What is HawkEye AP?”, next
- “HawkEye AP Components for Installation”, on page 14
- “HawkEye AP Concepts and Processes”, on page 15
- “Planning for HawkEye AP Configuration and Deployment”, on page 16

What is HawkEye AP?

HawkEye AP is a data analytics platform, providing an event data collection and event management solution to organizations faced with targeted threats to security that require forensic analysis and to organizations needing to comply with federal regulations that typically require regulatory analysis.

Among the features and capabilities of HawkEye AP are:

- **Security Intelligence**
  - Ability to perform sophisticated correlations and contextual investigations against large volumes of data over time.
  - An open access interface that lets users query event data directly from the Business Intelligence tools they prefer using ODBC/JDBC interfaces
  - Rich reporting and query capabilities including ad hoc reporting, predefined report templates for regulatory compliance, and customized reporting through console (dashboard) tools that provide flexible querying using Hexis Cyber Solutions own HawkEye AP SQL.
- **Event Data Collection**
  - Agent-less collection of any event with a time stamp
  - Open architecture that interfaces with a variety of related technologies, including endpoints and network systems, storage, mobile solutions, other SIEMs, call center applications, etc.
- **Event Data Warehouse**

  HawkEye AP’s clustered, columnar-based event data warehouse provides:

  - Ability to store all event data in its native form (rather than metadata, an aggregation, or a normalized form) ensuring integrity for future data use.
  - Real-time ability to access terabytes of event data, without the need to extract from any archive – allowing for rapid response to investigations and queries.

- Massively Parallel Processing (MPP) enables linear scalability in handling large data volumes in which highly compressed format reduces storage requirements.

The components that you will be installing that make these features possible are described below.

HawkEye AP Components for Installation

The following HawkEye AP Components are required for installation and together deliver a complete data analysis solution, from data loading and storage, to batch collection, rules management, and data analysis. Refer to Figure 1-1. Each component is described applicable section below:

- "HawkEye Event Data Warehouse (EDW)", next
- "Collector", on page 14
- "Analyzer", on page 14
- "Postgres and Open Access Extension", on page 15

HawkEye Event Data Warehouse (EDW)

The HawkEye Event Data Warehouse (EDW) component is a database built for and dedicated to loading, storing, and querying log entries. The software uses sophisticated, application-level clustering to perform all load and query tasks fully in parallel across any number of hosts. This architecture allows users to load and query massive data volumes in a single, logical database instance without partitioning. The EDW uses a patented mechanism that achieves high levels of compression, while still making all data fully available to query. This mechanism also removes the performance and storage overhead of indices on specific columns.

After installation, you add and configure one or more EDW instances on the hosts in your HawkEye AP deployment.

EDW LDAP

A standard HawkEye AP deployment authenticates and authorizes users through a private LDAP (Lightweight Directory Access Protocol) instance, `atslapd,` that is installed by default when you install HawkEye AP. HawkEye AP Analyzer and the `atmanage` command enables you to manage users and roles stored in this LDAP instance. HawkEye AP queries this LDAP instance to grant users access to HawkEye AP features and data.

Collector

The Collector component automates the collection and loading of event-log data into the Event Data Warehouse (EDW), either scheduled, on-demand, or in continuous mode. It supports standard interfaces, including TCP, FTP, SFTP, SCP, LEA, SMB, RCP, HTTP (Get and Push). It also provides status of retrieval and loading activities through the Analyzer and Collector activity logs

The installation procedure installs the Collector *and* configures its basic properties. After installation, you must configure Collector modules for each log source. For details, see the *Collector Guide*.

Analyzer

The Analyzer component lets authorized users view reports, alerts, and dashboards, manage assets, enable and disable Parser rules, run reports, schedule jobs, and manage users and roles. Command-line utilities also communicate with the Analyzer to access stored data and configuration information. The Analyzer is installed and configured during installation. For information about configuring the Analyzer, see the *Administration Guide.*

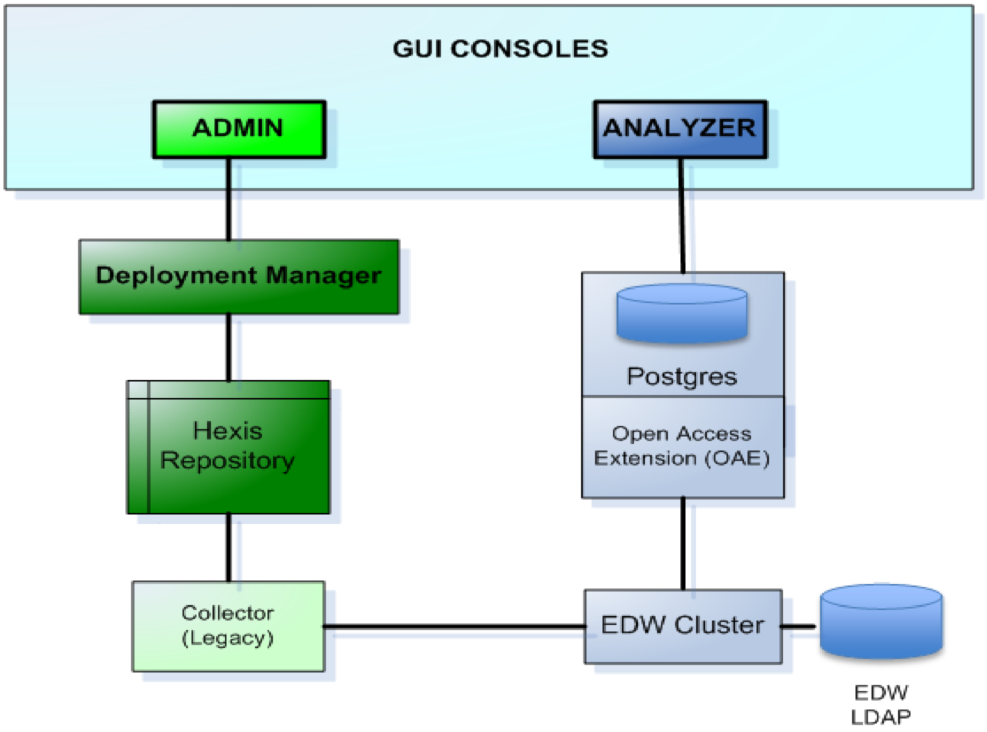
Postgres and Open Access Extension

When you install HawkEye AP, Open Access Extension (OAE) is also installed. OAE is an open interface that allows users to access EDW data with such open standards as ANSI SQL, ODBC, and JDBC. OAE uses the Postgres database query processing interface to provide access to HawkEye EDW data. By default, OAE is installed in `<HawkEye AP Home>` and places its executable files in:

```
<HawkEye AP Home>/bin
```

By default, the HawkEye AP home directory prefix is `/opt/hexis/hawkeye-ap/`.

Figure 1-1: The HawkEye AP Solution



HAWKEYE AP CONCEPTS AND PROCESSES

HawkEye AP, formerly Sensage's Log Management solution, delivers an unparalleled solution with the industry's most unique approach to analytics and intelligence – a flexible event data collection process and a clustered, columnar-based event data warehouse.

Data Collection

Your HawkEye AP system supports collection of batch events from log files and other event repositories maintained by network devices and software applications. The Collector polls data sources or repositories to retrieve event data, which it loads into the Event Data Warehouse (EDW). The EDW makes the event data available to the Analyzer for report management. For details, see the *Collector Guide*.

Data Transformation through Log Adapters

When the data is collected and before it is transported, it must undergo data transformation since the event logs contain events from a variety of hardware and software applications stored in different formats.

Customer-specified Log Adapters are available to transform these diverse events and format them into useful data for storage in the EDW. Log Adapters use PTL (Parse, Transform, Load) files to define the transformation of log data before they are stored in the EDW.

Hexis Cyber Solutions provides Log Adapters with your HawkEye AP distribution for a variety of common information systems and devices. See the *Analytics Guide* for all available Log Adapters. Customers can also create their own log adapters using the PTL format described in Appendix A of the *Collector Guide*.

Data Transport through Retrievers

The Collector loads data from a log file into an EDW table after parsing and transforming the log data through a PTL (Parse, Transform, Load) file. A log queue stores files while they are being downloaded or waiting for loading. The Collector sends the data to syslog-ng, which in turn makes it available for retrieval through a Retriever using one of the standard interfaces such as SFTP, FTP, etc.

PLANNING FOR HAWKEYE AP CONFIGURATION AND DEPLOYMENT

Your deployment of HawkEye AP comprises one or more hosts on which the HawkEye AP software runs. The HawkEye AP solution requires that you deploy the software on multiple hosts. Generally, the hosts that you allocate in your HawkEye AP deployment are for use by HawkEye AP software only. Other hosts in your computing environment lie outside your HawkEye AP deployment.

Because HawkEye AP supports a multiple-host deployment, you install the software on all HawkEye AP hosts, but you configure different components and modules to run on specific hosts within the deployment. Your specific HawkEye AP solution dictates the number of hosts in your overall deployment and the number of hosts within the deployment that you allocate to specific components and modules.

Multi-instance Support

By default, one EDW instance is set up on each EDW host during installation. To get better utilization of hosts with large number of cores and memory, you can run multiple EDW instances on each host.

Original installation

Additional EDW instances can be set up only during the original installation of the Hawkeye AP product. The same number of EDW instances are set up on each host within a Hawkeye AP 6.1.0 cluster, and that number cannot be changed after the original installation.

Extension

If the AP installation is extended with additional hosts for EDW, the same number of instances as set up in the original installation will be applied to the newly added hosts during the EDW extension process. For details on the extension procedure, see Chapter 4: Extending the Event Data Warehouse (EDW).

Upgrade

Upgrading from a Hawkeye AP 5.0.1 or AP 6.0.1 single-instance installation is supported. Upgrading from any multi-instance installation prior to AP 6.1.0 is not supported.

Deployment Manager

The Deployment Manager will guide you to install all components of the HawkEye AP product to your choice of hosts in your cluster with quick step-by-step screens and automated configurations. After installation, you can use the Deployment Manager to manage reconfigurations and operational needs of your HawkEye AP system. For example, the Deployment Manager console lets you add Collectors to your AP deployment, expand EDW hosts, monitor health of the cluster members, and start/stop specific AP services.

In addition, the Deployment Manager has an auto-update feature that polls the Hexis Repository for up-to-date released AP product RPMs. The Deployment Manager automatically downloads the new RPMs and updates its database about availability. You can see the available updates and can apply the updates at your convenience.

Master and Slaves

The master components are Analyzer, Open Access Extension (OAE), and Postgres, LDAP, used to manage all the other components in HawkEye AP. Note that there is only one instance of each master component in the HawkEye AP product. "Master" generally refers to a component that is installed on a single node, while "slave" applies to a component those that may be installed on multiple nodes. The slave components are EDW and Collector.

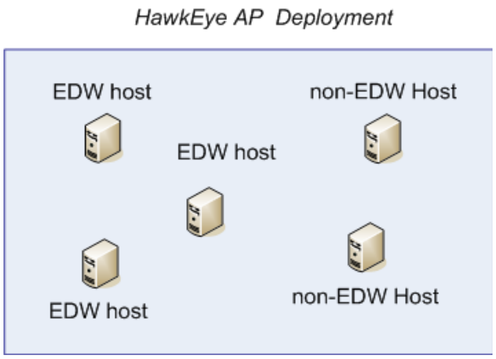
Hosts Component Planning

Plan your allocation of hosts carefully before you begin the installation and configuration procedures. Decide which hosts in your computing environment to allocate to your HawkEye AP deployment, and install HawkEye AP on all of them. Determine which hosts your HawkEye AP solution permits you to allocate to the EDW component and which hosts you can allocate to non-EDW components; add EDW instances and configure non-EDW components and modules accordingly.

EDW Hosts and HawkEye AP Product (Non-EDW) Hosts

In a multiple-host deployment, you allocate some hosts for use exclusively by the EDW component. You allocate the other hosts for use exclusively by HawkEye AP product (non-EDW) components. In the example deployment depicted in Figure 1-2, three hosts are allocated for the EDW component and two hosts are allocated to the HawkEye AP product components. The entire deployment comprises five hosts.

Figure 1-2: Host Allocation within a HawkEye AP Deployment



You allocate hosts within your deployment to the EDW and HawkEye AP product components during the configuration procedures. For example, you allocate hosts for the EDW when you add an EDW instance. You allocate hosts for HawkEye AP product components when you specify the hosts on which they run.

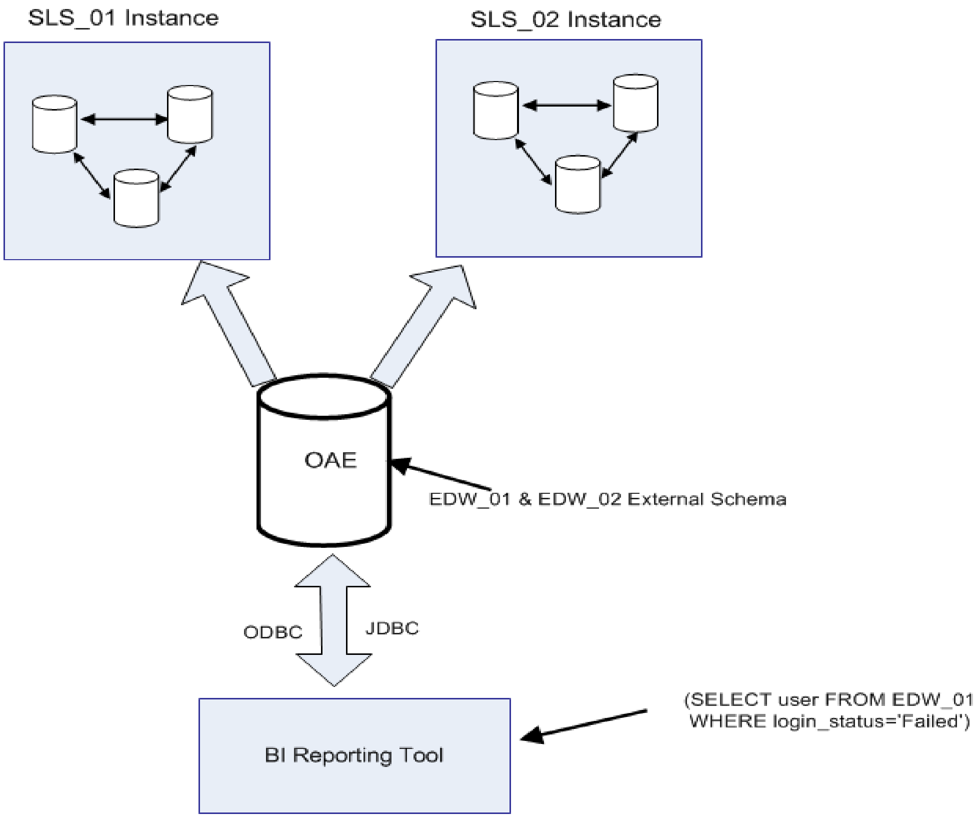
IMPORTANT: In your multiple-host deployment, do not add an EDW instance on hosts where HawkEye AP product components run, nor configure HawkEye AP product components to run on hosts where you added an EDW instance. The following components can and should run on non-EDW hosts:

- Analyzer
- Collector (Legacy)
- Postgres/OAE

Open Access Extension (OAE) in a Multi-cluster Environment

You can set up OAE to access multiple EDW cluster environments. For example, you can configure EDW clusters **EDW_01** and **EDW_02** on OAE by creating a connection to EDW, as well as an external schema of individual clusters in a single OAE environment. Then BI Reporting tools such as Pentaho can run join queries and access data from both EDW_01 and EDW_02 clusters. See Figure 1-3 below:

Figure 1-3: OAE in a Multi-cluster Environment



The requirements for setting up an OAE Multi-Cluster Environment are:

- Install and configure different EDW cluster instances

- Install and configure OAE or choose already installed and configured OAE from one of the HawkEye-AP cluster installations

For actual set up instructions, see “Setting up OAE for EDW Multi-cluster Access”, on page 208 of the *Event Data Warehouse Guide*.

CHAPTER 2

Preparing to Install HawkEye AP

Before installing HawkEye AP, you need to perform the following tasks.

- "Meet System and Product Availability Requirements", on page 15
- "Collect Information for the HawkEye AP Installer", on page 27

MEET SYSTEM AND PRODUCT AVAILABILITY REQUIREMENTS

This section contains HawkEye AP 6.2.0 Product Availability information. Review the sections below and their matrices to ensure your system meets all HawkEye AP-supported system and product requirements.

The topics in the following section include:

"Platform Support", next

"Architecture Support", on page 16

"Product Availability Matrix", on page 17

"OS Support", on page 19

"Data Collection Support", on page 19

"Virtualized Environments", on page 20

"System Hardware Requirements", on page 21

"End of Life Policy", on page 22

"Linux Configuration Recommendations", on page 22

"Linux Configuration Recommendations", on page 22

"Network Support", on page 23

"Required Ports for HawkEye AP 6.2.0", on page 24

"SAN and NAS Device Support (Optional)", on page 25

PLATFORM SUPPORT

Certified Platforms

Certified Platforms are those which Hexis has tested in Hexis testing labs, and are listed in the *Installation, Configuration and Upgrade Guide*, which is available on the Customer Support site. The certified platforms are summarized by the following table:

Server	Chip Type	Platform
Dell PowerEdge 2950	Xeon 50000-series	X86_64

Hexis supports the following hardware platforms to work with the HawkEye AP product suite:

Chip Type	Platform
Xeon 5000-series	X86_64
Opteron 2000-series	X86_64

Hexis no longer supports 32-bit hardware or 32-bit operating systems. All references to x86_64 are for Xeon or Opteron 64-bit processors. All references to ESX are for the specified OS running in the ESX environment (see below for detailed ESX requirements). Customers running older versions of HawkEye AP on 32-bit hardware should upgrade to HawkEye AP 4.6.3 which supports both 32 and 64-bit hardware with specific operating systems. On HawkEye AP 4.6.3 customers can migrate to newer hardware, then the system can be upgraded to HawkEye AP 5.0.1 and lastly to AP 6.2.0.

NOTE: Hexis supports Red Hat 5.x for upgrades only. Customers deploying new installations should choose a newer operating system. Customers should validate specific operating support for the hardware that is chosen for use with the HawkEye AP system.

Supported Platforms

Supported platforms are platforms explicitly listed in the Matrix below but have not actually gone through the automated testing process. These are platforms that Hexis Engineering has agreed to support based on their sole discretion that these platforms have no material difference from certified platforms. Both Certified and Supported platforms will be treated identically with respect to Support SLAs and Services.

Unsupported Platforms

Hexis will not provide any support for any operating system not explicitly listed in the "Product Availability Matrix", on page 17.

Architecture Support

Supported Architectures

Supported Architectures are those which Hexis has tested in Hexis testing labs, and whose complete configuration methodology is documented in this guide, which is available on the Customer Support site.

Unsupported Architectures

Unsupported architectures include any configuration of the product not explicitly documented in this guide, but which appear to work with customer experimentation. Customers running HawkEye AP software on unsupported architectures or configurations should be aware that they incur significant risk by doing so:

- Hexis Customer Support may not be able to provide any assistance with functionality related to the unsupported architecture. At their sole discretion they may continue to support the customer to the best of their ability.
- Customer Support will not entertain any requests for assistance with any issues regarding system performance in any area of the solution.

- Customer Support Response Times and SLAs only apply to licensed systems running in fully supported configurations. Due to the added complexity of problem resolution using the customer environment, Hexis problem resolution response time is likely to be longer than that for HawkEye AP Supported Architectures and configurations.
- Customer Support cannot escalate any issue to Hexis Engineering until the issue is reproduced on a fully supported architecture. The customer is ultimately responsible for reproducing the issue on a fully supported architecture. Therefore Hexis highly recommends customers maintain an additional representative test environment in a fully supported configuration.
- There is some chance that the issue will not be reproducible in a fully supported configuration. In this case the only next steps will be to change the customer configuration to a fully supported configuration.
- Hexis may or may not have roadmap plans for supporting the configuration in the future. If the product does later adopt support of the configuration, Customers may need to upgrade to a newer version of HawkEye AP. Such upgrades may not be automated or leverage any investment made in the previous environment.
- Hexis Professional Services may require the customer sign a letter stating acknowledgment of these risks before engaging in projects with unsupported configurations.

Product Availability Matrix

REVIEWER: PLEASE ADDRESS THE FOLLOWING: SS-13615 and SS-13894 FROM DAVE ABBOTT

The PAM states "HawkEye AP currently does not support use of other VMware tools such as but not limited to VMotion, DRS and HA." but this is now out of date as on page 210 of the EDW Guide in VMWARE MIGRATION we state that manual-mode DRS and HA has been tested. See SS-10542. VERIFY PAM NEEDS UPDATE

2. Can we get IC-1721 looked at so that we can fix the list of "REQUIRED PORTS FOR HAWKEYE AP 6.2.0" on page 30 ?

The following table details each of the HawkEye AP product components and the specific platform’s operating system combinations that those components can be installed and configured to run on. (See below for a table of which platforms HawkEye AP can collect data from). It is not intended to describe product functionality and capabilities. For information related to product functionality, see the HawkEye AP product documentation.

NOTE: This matrix shows 2015Q4 updates; HawkEye AP 5.0.1 was post-certified on RH 5.11, 6.6 and 6.7.

The letter "S" means it is fully supported. The string "U" means it is unsupported or known not to work, and blank spaces (no entry) are unsupported. Other strings are notes about specific versions that are fully supported only on those versions.

Additional Notes:

Windows Retriever requires NTLM v1 or NTLM v2 authentication. Note that support for Windows Retriever in this context refers to the platforms on which the Windows Retriever can run, as an agent or as part of the HawkEye AP Collector. This does NOT refer to the platforms from which the Analytics can retrieve and report on log data (see “Data Collection Support”, on page 19). Please review the documentation of the relevant Log Adapters or Report Packages for that information.

Java clients (Windows Retriever agent and HawkEye AP Analyzer) require JRE 1.6.0_45 or 1.7.0_80 and should have a minimum of 1GB of RAM.

The HawkEye AP Analyzer-supported include Internet Explorer 7, Internet Explorer 8, and Internet Explorer 9.

The HawkEye AP Storage Connector for EMC Centera uses version 3.2 patch 4 (64-bit) of the Centera SDK as a client. This Connector can be used with newer versions of Centera but only supports 3.0 functionality. The Connector can also be used with ATMOS version 2.1 or greater; however, there is no support for Retention or Retention Classes (as ATMOS does not support retention). The connector can also be used with ECS.

The HawkEye AP Storage Connector for Remote File Systems supports near-line storage via one of the following remote file system protocols: NFS v.3 or NVS v.4.

OS Support

New OS Releases

NOTE: At time of release, each HawkEye AP release will state in the Product Availability Matrix (PAM) which operating system updates will be supported. Based on market demand, on occasion but no more often than quarterly, Hexis may post-certify newer Red Hat releases on existing HawkEye AP releases. Hexis cannot make commitments in advance for specific releases for any specific quarter due to the nature of post-certification testing - we can only be sure a release will work when the tests pass.

If Red Hat issues a release with major security enhancements, security features or fixes, Hexis will incorporate that RH release into the next major or minor release of HawkEye AP (but not in HawkEye AP patch releases or hot-fixes).

Security Errata

For versions of Red Hat 5.7 and greater, HawkEye AP 6.2.0 is tested on a fully patched version of Red Hat as of the time of the HawkEye AP release. As Red Hat continues to release ongoing security errata Hexis will test these updates against the most recent patch release of HawkEye AP (e.g. 6.2.0) in a reasonable timeframe and will advise customers of any incompatibilities or other issues with the Red Hat updates.

NOTE: For releases of Red Hat before 5.7 Hexis supports only the kernels originally released in that version as per Red Hat's knowledge base: http://kbase.redhat.com/faq/docs/DOC-3079.

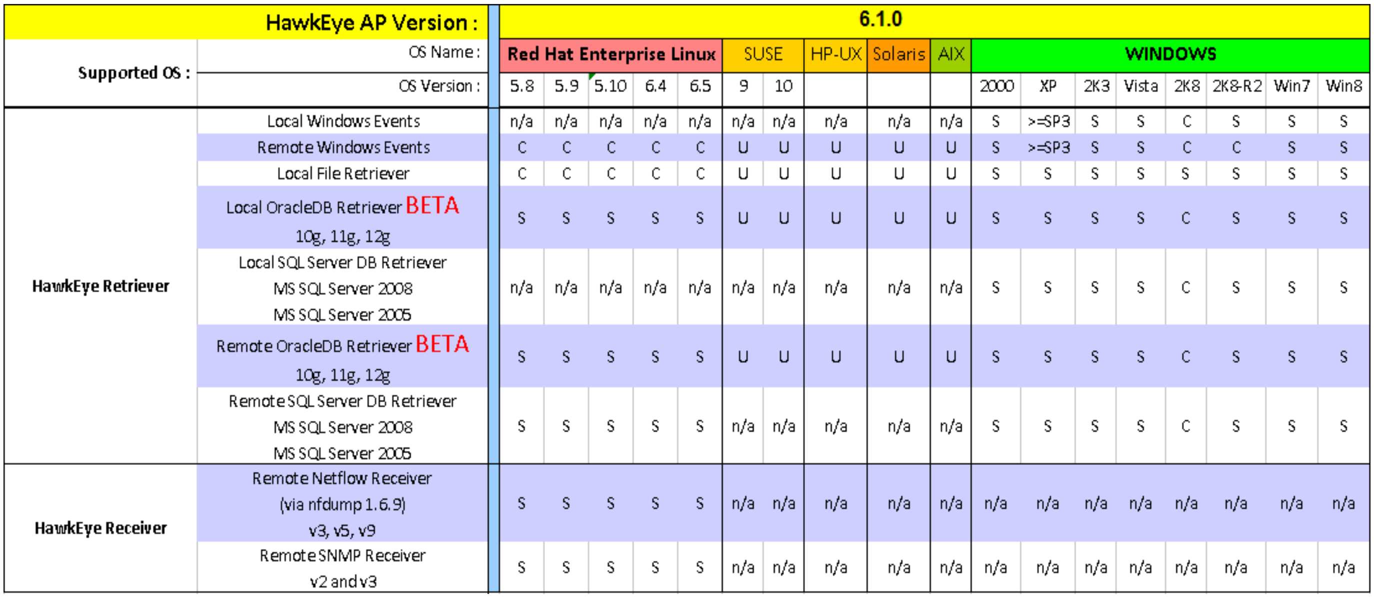
NOTE: Red Hat 4.x is no longer supported. Customers running older versions of HawkEye AP on Red Hat 4.x should upgrade to HawkEye AP 4.6.3 which supports specific updates of both Red Hat 4.x and 5.x. On HawkEye AP 4.6.3 customers can migrate the OS from Red Hat 4.x to Red Hat 5.x, and then the system can be upgraded to HawkEye AP 5.0.1 and lastly to 6.2.0.

Vulnerability Scanning

Each release of HawkEye AP is scanned with Nessus vulnerability scanner. See Release Notes for details of the environment setup and results of the scan. Customer requesting additional scanning with alternative scanners, for alternative environment setups, or for specific security requirements should contact Professional Services for analysis and scoping of that effort (this includes reviewing the results of scans performed by customers in their environments).

Data Collection Support

The following table details which platforms the HawkEye AP Collector and the HawkEye AP Retriever can collect data from. (See above for a table of which platforms each component can run on). For information regarding specific log files and formats from applications running on those platforms see the *Analytics Guide* product documentation.



HawkEye AP Version :		6.1.0																	
Supported OS :	OS Name :	Red Hat Enterprise Linux					SUSE		HP-UX	Solaris	AIX	WINDOWS							
	OS Version :	5.8	5.9	5.10	6.4	6.5	9	10				2000	XP	2K3	Vista	2K8	2K8-R2	Win7	Win8
HawkEye Retriever	Local Windows Events	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	S	>=SP3	S	S	C	S	S	S
	Remote Windows Events	C	C	C	C	C	U	U	U	U	U	S	>=SP3	S	S	C	C	S	S
	Local File Retriever	C	C	C	C	C	U	U	U	U	U	S	S	S	S	S	S	S	S
	Local OracleDB Retriever BETA 10g, 11g, 12g	S	S	S	S	S	U	U	U	U	U	S	S	S	S	C	S	S	S
	Local SQL Server DB Retriever MS SQL Server 2008 MS SQL Server 2005	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	S	S	S	S	C	S	S	S
	Remote OracleDB Retriever BETA 10g, 11g, 12g	S	S	S	S	S	U	U	U	U	U	S	S	S	S	C	S	S	S
	Remote SQL Server DB Retriever MS SQL Server 2008 MS SQL Server 2005	S	S	S	S	S	n/a	n/a	n/a	n/a	n/a	S	S	S	S	C	S	S	S
HawkEye Receiver	Remote Netflow Receiver (via nfdump 1.6.9) v3, v5, v9	S	S	S	S	S	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	Remote SNMP Receiver v2 and v3	S	S	S	S	S	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

The letter "C" means it is explicitly tested and supported. The letter "S" means it is untested; however, it is likely to work. The string "U" means it is not supported or known not to work. Other strings are notes about specific versions that have been tested and are fully supported on only those versions.

In this context the terms "Local" and "Remote" refers to the data being collected locally or remotely. Therefore for Retrievers "Remote" refers to either the default configuration with the Retriever running on the HawkEye AP Collector or with the Retriever installed as an agent on the specified OS, collecting data over the network from a remote source system. "Local" refers to the Retriever running as an agent on the source system. Receivers are only supported in the default configuration with the Receiver running on the HawkEye AP Collector.

NOTE: The special MS SQL Server 2000 functionality that includes collection of local files is not supported for remote connections to MS SQL Server 2000. For this functionality the Retriever must be installed locally on the source database server.

Virtualized Environments

Version Support

HawkEye AP has been certified to run on 64-bit VMware ESX (or ESXi) 4.1, 5.0, or 5.5.

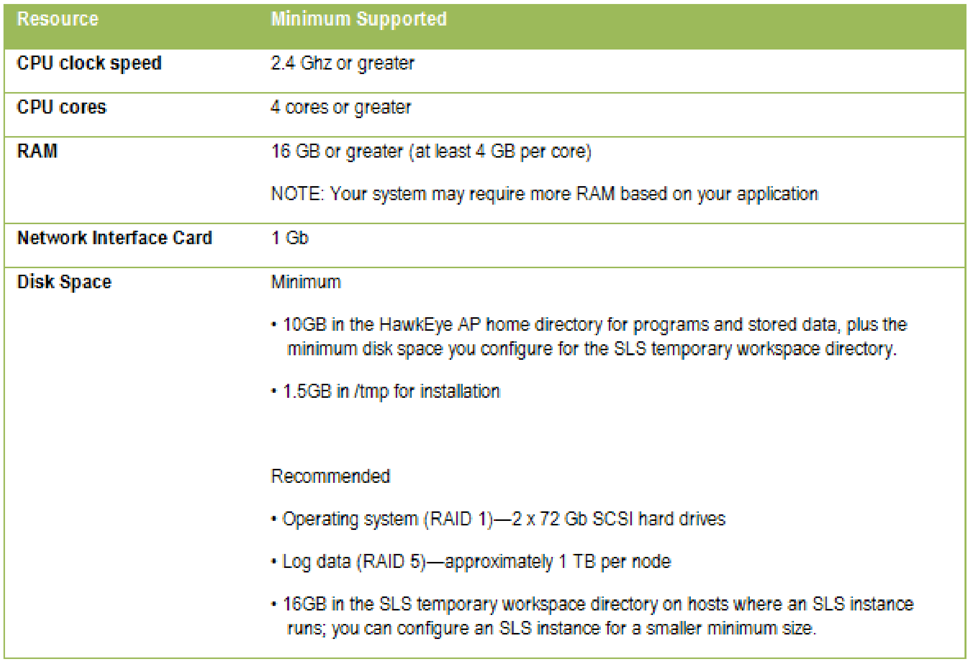
Virtualization Feature Restrictions

NOTE: Please review this list of VMware features that are NOT supported with HawkEye AP carefully before planning your deployment:

- HawkEye AP requires VMware ESX software version 4.1, 5.0, or 5.5.
- There is minimum 9-10% performance impact due to introduction of another software layer between HawkEye AP and hardware.

- Each instance of EDW, Collector, and Analyzer require a dedicated virtual machine with 4 physical CPU Cores mapped to exactly 4 virtual CPU cores.
- We recommend 16GB of dedicated memory to each virtual machine.
- System resource reservations are required.
- HawkEye AP component dedicated hardware must not be over-committed.
- HawkEye AP currently does not support use of other VMware tools such as but not limited to VMotion, DRS and HA.
- VMware trained staff to set up and manage the virtual environment.
- Each instance of HawkEye AP EDW requires 80 MB bandwidth to SAN with 100 IOPS.
- Use physical RDM since logical RDM results in additional 20% performance degradation
- One Gigabit NIC dedicated to each EDW in the cluster.
- Other recommendations/requirements are detailed in our documentation.

System Hardware Requirements



Resource	Minimum Supported
CPU clock speed	2.4 Ghz or greater
CPU cores	4 cores or greater
RAM	16 GB or greater (at least 4 GB per core) NOTE: Your system may require more RAM based on your application
Network Interface Card	1 Gb
Disk Space	Minimum • 10GB in the HawkEye AP home directory for programs and stored data, plus the minimum disk space you configure for the SLS temporary workspace directory. • 1.5GB in /tmp for installation Recommended • Operating system (RAID 1)—2 x 72 Gb SCSI hard drives • Log data (RAID 5)—approximately 1 TB per node • 16GB in the SLS temporary workspace directory on hosts where an SLS instance runs; you can configure an SLS instance for a smaller minimum size.

NOTE: The above Network and Disk requirements assume that each host will be using 4 cores. For larger hardware and solutions using more than 4 cores per host, additional network and disk bandwidth will be required. Note that only configurations for one NIC on each host are supported, therefore 10Gb NICs may be required. Please contact Hexis Professional Services for sizing and design of such solutions.

END OF LIFE POLICY

REMINDER: Customers should be aware of the end of life (EOL) policy in their end user license agreement. Typically this agreement stipulates that "Support and maintenance is provided for the current release and the immediately prior sequential release for a period of 12 months from the date of the current release".

With the release and public availability of HawkEye AP version 6.1.0 in September 2015, Hexis Cyber Solutions intends to phase-out version 5.0.x and plan for its EOL. Note that Hexis will continue support for version 5.0.x at least until September, 2016; when determined, the exact date for 5.0.x EOL will be publicized.

Further based on this policy support for version 4.0.x ended in November 2009, support for 4.1.x ended in June 2010, support for 4.2.x ended November 2010, support for 4.5.x ended February 2012, and support for 4.6.x ended October 2013.

Within each major release Hexis only supports the latest minor release. Therefore support for 5.0.0 ended with the introduction of 5.0.1.

LINUX CONFIGURATION RECOMMENDATIONS

The following is a list of recommendations when configuring Linux servers to host HawkEye AP.

1. Configure NTP (Network Time Protocol) for each server within the cluster. Establishing NTP enables accurate system times with consistent synchronization between nodes. Failure to configure NTP may result in problems with EDW.

2. For a large EDW cluster, resolving host names for the members of the EDW cluster locally improves both performance and reliability.

   a. Edit the file **/etc/nsswitch.conf** to put "files" as the first entry on the line that starts with "hosts:".

   b. Edit the file **/etc/hosts** to include the names and IP addresses of all the hosts that are part of the EDW cluster.

3. For EDW best performance, set the I/O scheduler to DEADLINE (kernel parameter in bootloader for **elevator=deadline**).

   NOTE: Because this setting allows the EDW to saturate the storage system, hosting of other services on the same servers that host the EDW is not recommended.

4. Avoid the use of "iptables", which can slow down networking performance and can cause spurious network failures under load (Packets are rejected when software-based iptables cannot keep up with network packet rate.).

5. Do not host EDW datastores on NFS shares because rapid create/delete/rename of files and directories in the EDW datastore often overwhelms NFS. Note, however, that you can host EDW datastores on NFS for nearline storage, which does not pose the same problem.

6. As a remedy for large EDW clusters experiencing spurious TCP connection failures try increasing "somaxconnto" in the /etc/sysctl.conf to a value equal to the number of cores in the cluster.

7. Your network topology should support full bandwidth between all pairs of EDW nodes. Choke points in the network topology can adversely impact performance (for example, when an EDW cluster splits into two pieces with a single 1Gbps link between the two halves).

8. Installation of the HawkEye AP product requires that you pre-install a set of Redhat RPMs or make them available for installation via a yum repo that is accessible during the HawkEye AP installation. For a list of RPMs that apply to the OS you are using, a tarball is provided in your installation, which provides three files for selected OS releases. When untarred, these files are stored in the hawkeye-ap/kickstart directory To untar the files and select the one that matches your OS release, perform the following steps:

   a cd <*your_choice_directory, for example, /tmp*>

   b Copy the tarball to this directory.

   c `tar xvzf` <*tarball_name*>.

   A subdirectory hawkeye-ap will be created.

   d `cd hawkeye-ap/kickstart`.

   Select the one that matches your OS release.

   The "yum" repo is also used to install the HawkEye AP product components. Because the "yum install" may find the non-HawkEye repo files first, you must configure each of the repos in the yum repos directory (**/etc/yum.repos.d/by default)** to continue the search in other repos files if the target was not located. To provide this configuration, add the following line to each enabled repo:.

   skip_if_unavailable = 1

   If all the required RPMs are already pre-installed, access to a local Redhat yum repo is optional.

NETWORK SUPPORT

HawkEye AP provides support for the following IP address formats.

- IPv4 only
- IPv6 only
- IPv4 and IPv6 mixed environment

HawkEye AP Components and the Networking Environment

Observe the following Networking requirements:

1. Every HawkEye AP component should have a valid networking route to any other component.
   - The routes can traverse IPv4 and IPv6 networks.
   - Both endpoints must have appropriate IPv4 and/or IPv6 addresses bound to their NICs.
2. The log collection components must have a valid networking route to any server/device from which they are collecting log data.
   - The routes can traverse IPv4 and IPv6 networks.

- Both endpoints must have appropriate IPv4 and/or IPv6 addresses bound to their NICs.

3. Hexis Cyber Solutions recommends the use of hostnames (as opposed to literal IP addresses) when configuring the HawkEye AP components.

   - This means that name resolution must be properly configured.

REQUIRED PORTS FOR HAWKEYE AP 6.2.0

The following ports are required for the HawkEye AP 6.2.0 deployment:

Deployment Manager without Ambari		
HawkEye AP YUM Repository	TCP 8081	Deploys RPM packages over HTTPS using Apache Web Server.
Secure Shell (SSH)	TCP 22	Automatically install and register Ambari clients.
HawkEye AP Update	TCP 7748	Automatic HawkEye AP product updates.
Ambari Server		
Secure Shell (SSH)	TCP 22	Automatically install and register Ambari clients.
Ambari Web	TCP 8443	
Ambari Agents	TCP 8440-8441 TCP 8443	Handshake, registration, and communication.
Ambari Postgres	TCP 5433	
HawkEye AP Hosts		
Ambari Agents	TCP 8440-8441	Handshake, registration, and communication
Secure Shell (SSH)	TCP 22	Needed to install Ambari client automatically and to execute prepare host script.
Collector Port	TCP 6677	
OAE/Postgres	TCP 5432	
Apache Tomcat: Advanced Analytics App Manager	TCP 8090 and 8005	Services provided by tomcat.
Apache Web Server: Ganglia Kibana	TCP 80 and 443	Services provided by Apache Web Server.
EDW/SLS	TCP 8072	
LDAP	TCP/UDP 30389	
Ganglia	TCP 8660 (collectors/slaves) TCP 61-63 (collectors) TCP 8651 (gmetad)	
Nagios	TCP 80	Nagios web interface used for clients and master.
Automatic Update	TCP 7748	Used to access automatic update yum repo.

SSL Setup

Connections to the Deployment Manager are protected by SSL, using a self-signed SSL certificate that is generated automatically during the installation process. The self-signed SSL certificate is set to expire three years from time of insallation. You can replace the automatically generated self-signed SSL certificate with your own certificate. For details on this and managing the SSL certificate, see, “Using a Custom SSL Certificate for Deployment Manager”, on page 38 in the *Administration Guide.*

SAN and NAS Device Support (Optional)

Hexis Cyber Solutions provides support for both Storage Area Network (SAN) and Network-Attached Storage (NAS). Both SAN and NAS forms of storage allow for data sharing through a LAN network connection.

- With SAN, storage is available through a server or other dedicated hardware device at a block-level. Metadata changes, along with any other updates, are simply processed as read/writes to blocks on disk,
- With NAS, storage is available through a connection to a dedicated server at the file-level. NAS is suitable only for hosting nearline storage. For details, see Chapter 9: Archiving to Nearline Storage in the *Administration Guide*.

NAS devices are unsuitable for use as on-line storage for the EDW data store. This is because at times it cannot keep up with the rate at which the EDW makes metadata changes in the file system and it must process metadata changes in a special manner that takes a considerable time to complete. For a NAS sharing a file system, metadata changes are special operations that require synchronization across hosts, etc.

The following section provides requirements and considerations when using SAN to host Enterprise Data Warehouse (EDW) storage.

Storage Area Network (SAN) EDW-Hosting Requirements and Considerations

SAN devices for hosting EDW on-line storage is supported in a configuration in which a SAN device has LUNs (remote block devices) to host systems. In this configuration, LUNs are mounted on host systems and a standard ext3/ext4 is built within the LUNs to support the on-line data store. Each LUN is mapped to a single host. Note that ext3/ext4 is not a clustered file system and therefore, it cannot be shared at the block device level among multiple hosts.

Storage Performance

SAN devices support Hexis-documented throughput and latency requirements (80 MBps/node and 100 IOPS/node) for the HawkEye AP product. These throughput and latency requirements apply to both the SAN device and whatever communication paths are set up between the hosts and the SAN. Note that SAN device performance requirements, however, do not consider how mapping is applied from the raw disk to the LUNs.

Data Compression

- SAN-side compression to conserve raw disk does not provide a gain in effective storage capacity and may impact performance.
- The EDW compresses data prior to writing the data to disk, which makes storage-level compression ineffective.

- SAN-side de-duplication is unlikely to show much of an improvement in terms of conserving disk space and may represent a performance penalty.

Data Encryption

- SAN-side encryption may have a performance impact; it does not provide protection similar to EDW data-at-rest encryption. The possible performance impact depends on how the SAN device implements the encryption.
- SAN-side encryption protects the contents of the drives should they be removed from the SAN device; however:
  - It does not protect the contents of the disk from inspection, replication, and modification by processes running on the customer's site.
  - It does not protect the contents of files which are copied off the disks while the SAN is running.
- EDW data-at-rest encryption protects the EDW data files themselves, prohibiting other processes from reading or modifying data file contents. This applies to processes running at the customer's site and processes running off-site against copies of the EDW data files.

Data Replication

- Most SAN customers turn off EDW replication and rely on the fault tolerance of the SAN to safeguard the data.
- Turning off EDW replication means the EDW cluster cannot function if one or more EDW nodes are down.
- When an EDW node fails and replication stops, the EDW cluster cannot function if one or more EDW nodes are down.
- With no replication, when an EDW node fails, there is no way for the cluster to access that node's shard of the collective data store.

Hierarchical Storage

- SAN-side "hierarchical" storage or "tiering" does not, in general, cause problems:
  - Migration of data from one tier to another should not impact performance; however, be sure to consider whether the SAN device can migrate data without impacting the performance of ongoing activities.
  - EDW activities which require data that has been moved to a slower tier may slow performance impact.

Replication, Snapshots, and Backups

- SAN-level replication, snapshots, and backups are not guaranteed to capture a consistent image of the EDW data store as these activities may occur while the EDW is in the middle of modifying its data store.
- A consistent image of the EDW data store is ensured when the SAN's operation is guaranteed to capture the entire state of the entire block device at a single point in time. However, even with a guaranteed atomic snapshot of the entire LUN the default journaling in Linux for ext3/ext4 only ensures that the metadata on disk is consistent. This means that a block-level snapshot may be missing the contents of some files which gives one a corrupted EDW data store in replication.

- If the EDW is not processing changes and the Linux file system cache has written to disk, then an atomic block-level replication will be successful.

COLLECT INFORMATION FOR THE HAWKEYE AP INSTALLER

Refer to Appendix A, which provides a check list of information that the HawkEye AP Installer will request during installation. Keep the checklist on hand before you run the installer.

CHAPTER 3

Installing and Configuring HawkEye AP

This chapter provides step-by-step instructions for installing, configuring, and deploying HawkEye AP using the HawkEye AP Installation Wizard. It contains the following sections:

- "Before You Begin the Installation", on page 35
- "Install, Configure, and Deploy HawkEye AP", on page 42
- "Verify Your Installation", on page 53
- "Perform Post-Installation Tasks", on page 54
- "Optional: Installing HawkEye AP with the Deployment Manager Tool", on page 56

IMPORTANT: This chapter assumes you have determined your configuration and prepared for your installation as described in Chapters 1 and 2 of this guide.

BEFORE YOU BEGIN THE INSTALLATION

This section provides information you need to know before beginning the installation. This section contains the following topics:

- "General Install Pre-checks and Restrictions", on page 36
- "Configuring HawkEye AP Cluster for Auto-Updates", on page 38
- "Performing Auto-Update for HawkEye AP Components", on page 39
- "Performing Manual Update for HawkEye AP Components", on page 41
- "Component Install Restrictions", on page 41
- "Installation Overview", on page 41
- "About the HawkEye AP 6.2.0 Software Package", on page 42

General Install Pre-checks and Restrictions

This section contains a checklist to ensure you have met prerequisites and are aware of restrictions before beginning the install.

SOFTWARE PACKAGES

Double check the list of software packages installed before proceeding with installation of AP. The list of software packages is listed in the tar-ball of the software. To perform the check:

1 Select the appropriate kickstart file within the tarball under **hawkeye-ap/kickstart/ directory**.

File Name	Supported OS
el5-packages	All EL5
el64	EL 6.0 - 6.4
el65	EL 6.5

2 Copy the packages file to the appropriate hosts:

```
scp <file> root@<host>:/tmp/
```

3 SSH into the host you copied the file above to:

```
ssh root@<host>
```

4 Execute the following to validate package list

```
rpm -q `grep -v ^-  /tmp/el64-packages` | grep 'not installed'
```

5 Install any missing RPMs as root user

```
yum install <rpm>
```

Configuration

When using any version of Red Hat Enterprise Linux, the default **ssh_config** file causes **clssh** commands to fail when there are too many concurrent server connections in a short time span. To work around this limitation, set the **MaxStartups** parameter to **1000** (the default is **10**). This parameter is related to three other settings. For further details on this setting, see *https://en.wikibooks.org/wiki/OpenSSH/Cookbook/Load_balancing.*

Logging

While verbose logging is helpful in diagnosing certain problems, for performance reasons do not set verbose logging by default during the install. If you see any issues after the cluster is running, only then change the logging level to verbose to get more detailed information.

Snappy 'package

Before starting the install, check and remove the package "snappy" if it is already installed on any of the host(s) in the cluster. Failure to do so will cause an installation error.

1 Run the below command to check if "snappy" is installed:

```
rpm -qa | grep snappy
```

2 Remove if "snappy" is already installed.

For example: `yum remove snappy`

Parameter Restrictions

Once configured during the installation, the following parameters *cannot* be changed.

Component	**Parameter(s)**
OAE Database	OAE data directory
EDW LDAP	LDAP domain LDAP data directory
EDW	EDW data directory EDW Port EDW Instance Name
Advanced EDW	NSS cache directory NSS ID list file NSS NSI list file NSS socket file EDW data mirroring
Collector	Collector data directory
General	HawkEye AP install directory

Clusters with Many Nodes

If you have a cluster with many nodes, you should add the file **/etc/security/limits.d/91-nagios.conf** to the Nagios server host and reboot the Nagios server host *BEFORE* running the host registration step, "Select Install Options", on page 44, in the Deployment Manager GUI.

If you do not do this and Nagios reverts to a down state despite your repeated attempts to start it, then you can add the file /**etc/security/limits.d/91-nagios.conf**, and reboot the Nagios server host before starting Nagios from the Deployment Manager.

Steps for adding **/etc/security/limits.d/91-nagios.conf** to the Nagios server host:

1 Add a file **/etc/security/limits.d/91-nagios.conf** on the Nagios server host with following contents:

```
nagios hard nofile 1000000
nagios soft nofile 100000
nagios hard nproc 100000
nagios soft nproc 4096
```

2 Reboot the Nagios server host.

3 After the reboot, it may take a few minutes for the Deployment Manager to get the heartbeat from all the hosts in the cluster again. All the components are functional despite the "No Heartbeat" status during this time.

Configuring HawkEye AP Cluster for Auto-Updates

Updated HawkEye AP product RPMs will be made available at:

```
http://support.hexiscyber.com:7748/hawkeye-ap/
```

Access to this URL is restricted based on your organization’s IP address. To gain access, contact Hexis Support and provide the IP address of the system that will be used to access the updated RPMs.

There are three configurations available for accessing the updated RPMs depending on your security policies.

The easiest option is to allow the Deployment Manager to access the support site either directly or through a proxy server.

Refer to your applicable case below and follow the configuration steps.

Case 1. Direct Access to the Hexis Support Site

To have Deployment Manager directly access the Hexis support:

1 Get access to the RPMs by informing Hexis Support of Deployment Manager's IP address.

2 On Deployment Manager copy **/opt/hexis/hawkeye-ap/sync -rpms/hexis.rhel[5|6].repo** to **/etc/yum.repos.d/hexis.repo**

3 Enable the sync-rpms cronjob by editing **/etc/cron.d/sync-rpms.cron** and uncommenting the job. The execution time and frequency may also be adjusted.

4 See “Performing Auto-Update for HawkEye AP Components”, on page 39 to continue the process.

Case 2. Access to the RPMs through Proxy Server’s IP Address

Get access to the RPMs by informing Hexis Support of the proxy server's IP address:

1 On Deployment Manager copy **/opt/hexis/hawkeye-ap/sync -rpms/hexis.rhel[5|6].repo** to **/etc/yum.repos.d/hexis.repo**.

2 Edit **/etc/yum.repos.d/hexis.repo** to update the URL to go through the proxy server.

3 Enable the sync-rpms cronjob by editing **/etc/cron.d/sync-rpms.cron** and uncommenting the job. The execution time and frequency may also be adjusted.

4 See “Performing Auto-Update for HawkEye AP Components”, on page 39 to continue the process.

Case 3: Mirror the updated AP Product RPMs on a Local Yum Server

To mirror the updated HawkEye AP product RPMs on a local yum server to which Deployment Manager has access:

1 Get access to the RPMs by informing Hexis Support of the local yum mirror's IP address.

2 Configure the local yum mirror to mirror the Hexis support site.

3 On Deployment Manager copy **/opt/hexis/hawkeye-ap/sync -rpms/hexis.rhel[5|6].repo** to **/etc/yum.repos.d/hexis.repo**.

4 Edit **/etc/yum.repos.d/hexis.repo** to change the URL to the local yum mirror.

5 Enable the sync-rpms cronjob by editing **/etc/cron.d/sync-rpms.cron** and uncommenting the job. The execution time and frequency may also be adjusted.

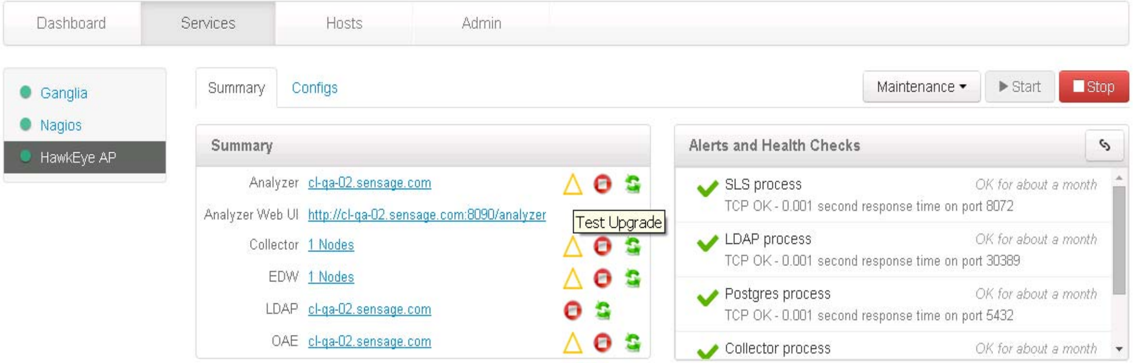
6 See “Performing Auto-Update for HawkEye AP Components”, on page 39 to continue the process.

Performing Auto-Update for HawkEye AP Components

To perform auto-update of HawkEye AP components, perform these steps:

1 Log into Deployment Manager and click HawkEye AP.

2 Click the Yellow triangle icon next to the selected component to perform Test Upgrade on the component.



Analyzer	cl-qa-02.sensage.com
Analyzer Web UI	http://cl-qa-02.sensage.com:8090/analyzer
Collector	1 Nodes
EDW	1 Nodes
LDAP	cl-qa-02.sensage.com
OAE	cl-qa-02.sensage.com

SLS process — OK for about a month
TCP OK - 0.001 second response time on port 8072

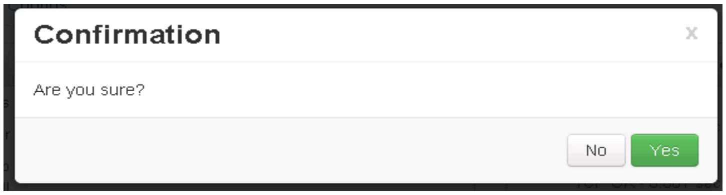
LDAP process — OK for about a month
TCP OK - 0.001 second response time on port 30389

Postgres process — OK for about a month
TCP OK - 0.001 second response time on port 5432

Collector process — OK for about a month

NOTE: The sequence of upgrade must be followed in this order: LDAP, EDW, OAE, and the Collector, Analytics, and Analyzer. If the triangle icon is not available, this means there is no available updates for this component. You can skip to the next available upgrade in the sequence.

3 Click **Yes** to confirm the upgrade.


Confirmation

Are you sure?

The Background Operations list is displayed, showing a list of operations.

4 Click the operation that is listed for "Testing Upgrade" of the component that you selected.

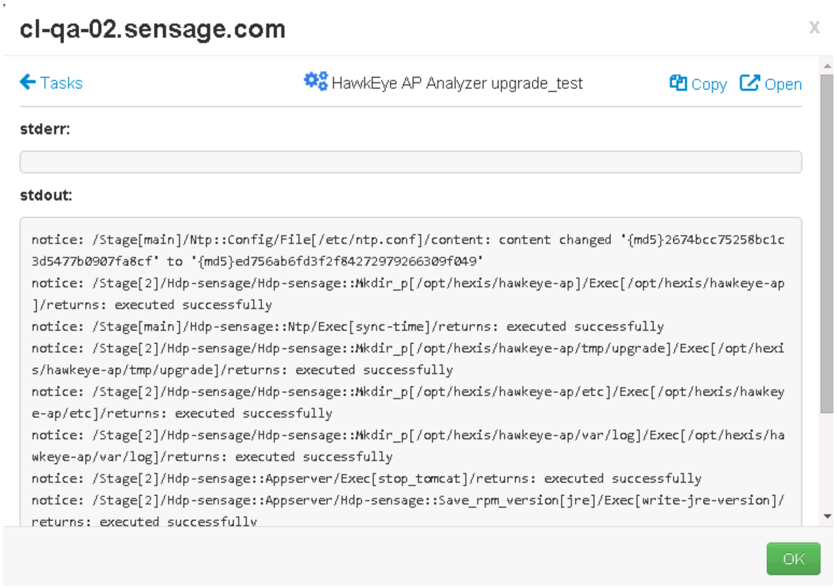
The Host list is displayed.

5 From the Host list, click the desired host for the component you selected.

The Task list is displayed.

6 From the Task list, click the task on the list.

The Test Upgrade information is displayed in **stderr** and **stdout** format.



cl-qa-02.sensage.com

stderr:

stdout:

```
notice: /Stage[main]/Ntp::Config/File[/etc/ntp.conf]/content: content changed '{md5}2674bcc75258bc1c
3d5477b0907fa8cf' to '{md5}ed756ab6fd3f2f84272979266309f049'
notice: /Stage[2]/Hdp-sensage/Hdp-sensage::Mkdir_p[/opt/hexis/hawkeye-ap]/Exec[/opt/hexis/hawkeye-ap
]/returns: executed successfully
notice: /Stage[main]/Hdp-sensage::Ntp/Exec[sync-time]/returns: executed successfully
notice: /Stage[2]/Hdp-sensage/Hdp-sensage::Mkdir_p[/opt/hexis/hawkeye-ap/tmp/upgrade]/Exec[/opt/hexi
s/hawkeye-ap/tmp/upgrade]/returns: executed successfully
notice: /Stage[2]/Hdp-sensage/Hdp-sensage::Mkdir_p[/opt/hexis/hawkeye-ap/etc]/Exec[/opt/hexis/hawkey
e-ap/etc]/returns: executed successfully
notice: /Stage[2]/Hdp-sensage/Hdp-sensage::Mkdir_p[/opt/hexis/hawkeye-ap/var/log]/Exec[/opt/hexis/ha
wkeye-ap/var/log]/returns: executed successfully
notice: /Stage[2]/Hdp-sensage::Appserver/Exec[stop_tomcat]/returns: executed successfully
notice: /Stage[2]/Hdp-sensage::Appserver/Hdp-sensage::Save_rpm_version[jre]/Exec[write-jre-version]/
returns: executed successfully
```

7 Click **OK**.

In the Services tab under the Summary section, you will see the component that you just upgraded with two new icons beside it. One icon represent Apply Upgrade (checkmark symbol) and the other is Revert Upgrade (with an "X" symbol).

8 After you have made sure the Test Upgrade is 100% complete, click checkmark symbol for **Apply Upgrade**.

9 Click **Yes** to confirm.

The Operation will list the "Apply Upgrade to the Component" that you selected.

10 If desired you may click for futher information as in steps 4, 5, and 6 above.

11 Repeat the step for each component that you want to upgrade, in keeping with the sequence of components required for upgrade, noted in Step 2.

If the triangle icon is not available, this means there are no available updates for this component. You can skip to the next available upgrade in the sequence noted above until you have upgraded all desired components.

Performing Manual Update for HawkEye AP Components

Another alternative is to manually download the updated HawkEye AP RPMs and copy them onto the Deployment Manager. With this option, updates will not show up on the web UI. hawkeye-deploy must be used to perform upgrades.

1 Get access to the RPMs by informing Hexis Support of the IP address of the local system that will be used to download the RPMs.

2 Download the updated RPMs.

3 Copy the updated RPMs onto Deployment Manager into a directory under **/var/www/html/hawkeye-ap/hawkeye-ap**. Updated RPMs may be placed directly into /**var/www/html/hawkeye-ap/hawkeye-ap** or updates may be organized by creating subdirectories such as **/var/www/html/hawkeye-ap/hawkeye-ap/edw_6.2.0**.

4. Update Deployment Manager's yum repo metadata by using the applicable command below.

a On a rhel6 system, to produce repo for rhel6, execute:

```
createrepo --update /var/www/html/hawkeye-ap/hawkeye-ap
```

b On a rhel6 system, to produce repo for rhel5, execute:

```
createrepo -s sha1 --update /var/www/html/hawkeye-ap/hawkeye-ap
```

c On a rhel5 system, to produce repo for rhel5, execute:

```
createrepo --update /var/www/html/hawkeye-ap/hawkeye-ap
```

NOTE: Redhat recommends against using createrepo on a rhel5 system to produce repo for rhel6.

5. Use hawkeye-deploy to perform the upgrade.

Component Install Restrictions

The following are component install restrictions to note when installing HawkEye AP 6.2.0.

Analyzer

OAE and Analyzer (the GUI) must be installed on the same machine. Note that by default, the installer will have you install the Analyzer on OAE and you cannot change to a different host.

EDW LDAP

LDAP setup and configuration is managed only at install time by the Deployment Manager.

Installation Overview

The first phase of HawkEye AP installation includes running an installation script to install the HawkEye AP Deployment Manager. The dependent Redhat RPMs are also installed on all the hosts.

In the second phase of the HawkEye AP installation, you enter the URL of the Deployment Manager in your web browser to start the Deployment Manager GUI, which guides you to install HawkEye AP components on all the hosts.

After installation completes, you can use the Deployment Manager GUI to start/stop AP components, add collectors, expand EDW hosts, and monitor health of the components and hosts. For details on the operation of this console, see the *Administration Guide*.

The installation script and Deployment Manager are available once you have downloaded the installation software, described in the following section. Read through the remainder of this section for more information on installation script options and installation files and directories.

About the HawkEye AP 6.2.0 Software Package

The software package for the HawkEye AP solution are available from the Hexis Cyber Solutions Technical Support Web site. When you extract the packages from the distribution tar file, the following is created: an installation utility for you to run, and a few other files. The staging directory is created underneath the current directory when you extract the contents of the tar file.

Installation Files and Directories

The installer places all files related to the HawkEye AP application in the directory tree under `/opt/hexis/hawkeye-ap`. The Datastore Root, which contains EDW data is set to `/opt/data/sls/<instance_name>/dsroot` and cannot be changed.

- Java is installed under `/etc/.java`, and `/usr/java`.
- syslog-ng is in a standard location under `/.` and `/etc/init.d/syslog-ng` is the actual daemon script.
- The following files are contained in the `/etc/init.d` directory:

ambari-agent	sensage_atpgsql
gmetad	sensage_atslapd
gmond	sensage_collector
hdp-gmetad	hdp-gmond
sensage_nss	nagios
sensage_sls_<*instance_name*>	

- The syslog-ng configuration file "syslog-ng.conf" is in a standard location under `/etc/syslog-ng/`.
- `/etc/init.d/syslog-ng` is the actual daemon script.

Install, Configure, and Deploy HawkEye AP

The HawkEye AP Deployment Manager installs, configures, and deploys HawkEye AP hosts along with required and optional components.

You start by installing the Hawkeye AP Deployment Manager. After that, you can use a web-based GUI client to tell the Deployment Manager which HawkEye AP version should be installed, and how it should be configured. HawkEye AP requires certain Redhat RPMs. These Redhat RPMs will be installed from the

Redhat repos that you have configured in `/etc/yum.repos.d/*.repos`, if these RPMs are not pre-installed.

The selected HawkEye AP components will be installed on the nodes you designated. At the end of the installation, the installed components will be automatically started.

Installing the Deployment Manager

IMPORTANT: If the installation of AP is interrupted for any reason (power failure, user changes his/her mind on the installation, etc.), you must uninstall AP prior to any future attempts to install AP again.

This section assumes that you have acquired your HawkEye AP software package. To install the Deployment Manager:

1 Login as root on a host with network access to all of the hosts where the HawkEye AP product will be installed.

2 Set up keys for ssh authentication. You can use ssh-keygen to generate the keys:

```
ssh-keygen
```

3 Extract the following tarball, which places the files into the **hawkeye-ap** directory.

```
hawkeye-ap-20140326-0929_el6-83141.tar.gz
```

4 Change the directory to the **hawkeye-ap**.

```
cd hawkeye-ap
```

5 At the prompt, run the installation script to start the installation of the Deployment Manager.

```
./install.sh
```

6 You will be asked to read the Hexis EULA. Press **ENTER** to proceed.

You can use the arrow keys to navigate the EULA.When you are satisfied, you can type **q** to continue.You will then be asked if you accept the EULA or not.Type **y** to continue with the installation, or type **n** to exit.

After installing the required Redhat RPMs, you will be informed of your Deployment Manager host configuration and details of the Deployment Manager installation. Press **ENTER** to proceed.

The Deployment Manager uses certificates to communicate with the other hosts where the AP components will be installed. The certificates are issued based on the current time. If the installation script cannot synchronize the time on the Deployment Manager host with an NTP server, you will be prompted to verify the current time. If the system clock is not correct, you must change the system clock to the correct value before proceeding. Failure to do so may result in subsequent AP component failures due to an invalid certificate. Press **ENTER** to continue after confirming that the current time is correct.

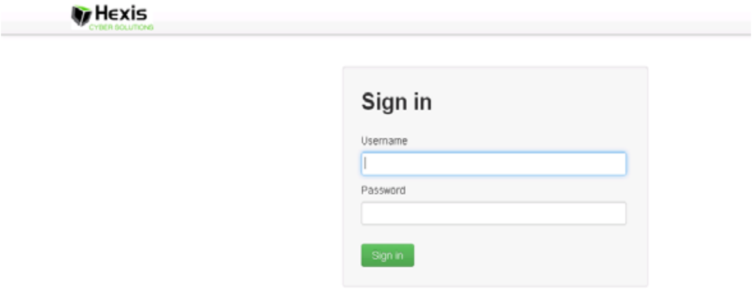
When the script completes, the Deployment Manager has been installed. You can access the Deployment Manager via a web browser using the URL printed by the script. Installing the HawkEye AP components using the Deployment Manager is an interactive process.

7 The Installer prompts you to verify the installation components. Press **Enter** to proceed.

Installing the HawkEye-AP Components

To begin the installation of HawkEye AP components, login to the Deployment Manager Installer:

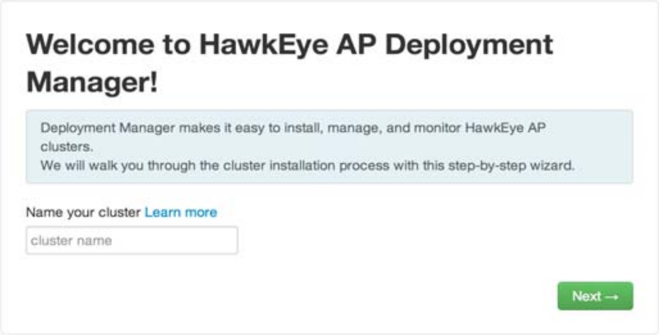
1 Sign into the HawkEye AP Installer using **admin/changeme** as the username/password. You can change this password at any time.



2 Click **Sign In**.

Name the HawkEye AP Cluster

1 At the HawkEye Welcome Screen, shown below, enter the name of the cluster that you want to create.



Welcome to HawkEye AP Deployment Manager!

Deployment Manager makes it easy to install, manage, and monitor HawkEye AP clusters.
We will walk you through the cluster installation process with this step-by-step wizard.

2 Click **Next**.

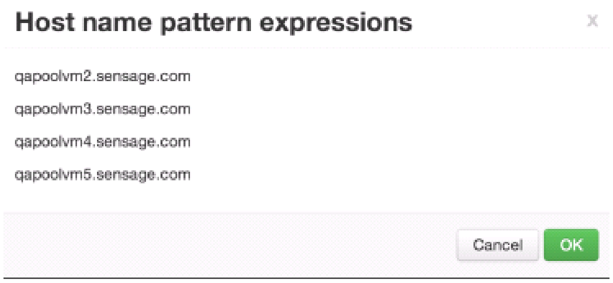
Select Install Options

In the Install Options screen, the Deployment Manager asks you for information required to set up your cluster; that is, configure your host registration.

IMPORTANT: If you have many nodes in your cluster, see *“Clusters with Many Nodes”, on page 37*.

1 Enter the target host(s) on which you are deploying the product as shown in the screen example below.

If you use a pattern expression to provide the hosts, the system displays a popup with an expanded list of host(s) as shown below.



Host name pattern expressions

qapoolvm2.sensage.com

qapoolvm3.sensage.com

qapoolvm4.sensage.com

qapoolvm5.sensage.com

2 To allow the Deployment Manager to configure all the hosts in the system, perform one of the two options during the host registration step:

Option 1:

- Provide the SSH private Key of the root user on the Deployment Manager host, AND
- Either provide the root password to access all hosts in the system, or set up the SSH trust among root accounts on all the hosts manually.

  For details, see Option 1 Registration Instructions below.

-OR-

Option 2:

- Perform the manual registration in **“Option 2 Registrations Instructions”, on page 45**.

OPTION 1 REGISTRATION INSTRUCTIONS

To provide the SSH Private Key:

The SSH private Key is in the file **/root/.ssh/id_dsa** or **/root/.ssh/id_rsa**. You can cut and paste the content of the file containing SSH Private Key into the GUI or you can specify the location of the file. By default, this is pre-filled in with the content of the SSH Private Key file found on the Deployment Manager host.If you are using Internet Explore 9, the Choose File button may not appear. Use the text box to cut and paste your private key manually.

To set up SSH trust for the root user (if not providing the root password to access all hosts in the system):

Add the root user's public key (from the file **id_rsa.pub** or **id_dsa.pub**) from the Deployment Manager host to the **/root/.ssh/authorized_keys** file (not authorized_hosts file) on each host that AP components will be installed on.

OPTION 2 REGISTRATIONS INSTRUCTIONS

If you decided to perform the manual registration, you do not have to set up SSH trust or provide a root password for the Deployment Manager host.

- The system will notify you that you must install Ambari Agents on each host you want to manage before you proceed.
- To do this, you must perform the following procedure on every host in your cluster so that Ambari Agent is installed on each host:

- **a** Copy the file **/etc/yum.repos.d/ambari.repo** from this server to your host's **/etc/yum.repos.d/** directory.
- **b** Copy the file /**var/lib/ambari-server/prepare-host.tar.gz** from this server to the **/tmp** directory on your host.
- **c** Extract the prepare host scripts on your host:

```
mkdir /tmp/prepare_host
tar zxvf /tmp/prepare-host.tar.gz -C /tmp/prepare-host
```

- **d** Run the prepare host scripts on your host:

```
/tmp/prepare_host/prepare_host.sh Ambari_Server_FQDN
```

- **e** Install lms-ambari-agent on the host:

```
yum install lms-ambari-agent
```

- **f** Configure the Ambari Agent by editing the ambari-agent.ini file and set the hostname to the FQDN of this ambari server

```
vi /etc/ambari-agent/conf/ambari-agent.ini
```

You should change "localhost" in the following to the fully-qualified domain name of your Deployment Manager host:

```
[server]
hostname=localhost
```

- **g** Start the ambari agent to automatically register this host to the server:

```
ambari-agent start
```

3 Click **Register and Confirm**.

Confirm Hosts

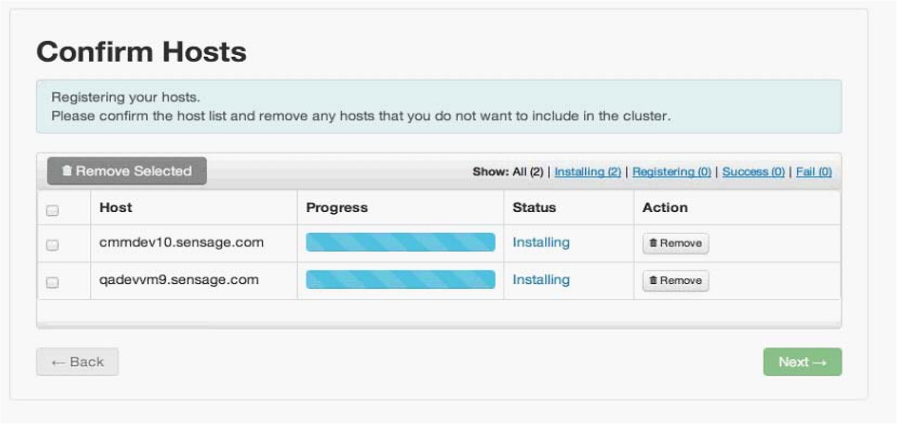
1 In the Confirm Hosts screen (shown below) confirm that HawkEye AP has located the correct hosts for your cluster and at the end of the list, click to check results.

NOTE:

- You can remove any host by selecting the appropriate check boxes and clicking the gray Remove Selected button. To remove a single host, click **Remove** in the Action column.
- During the check process, a yellow box indicates some warnings were encountered during the check process. Click to see a list of what was checked and what caused the warning.

2 If any hosts were selected in error, you can remove them by selecting the appropriate check boxes and clicking the gray **Remove Selected** button. To remove a single host, click the small white Remove button in the Action column.

3 When you are satisfied with the list of hosts, click **Next**.



Confirm Hosts

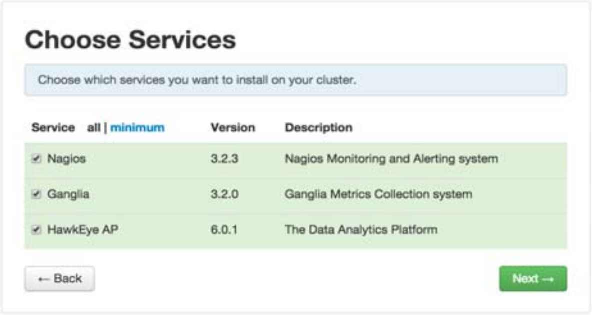
Registering your hosts.
Please confirm the host list and remove any hosts that you do not want to include in the cluster.

Remove Selected
Show: All (2) | Installing (2) | Registering (0) | Success (0) | Fail (0)
← Back
Next →

□	Host	Progress	Status	Action
□	cmmdev10.sensage.com		Installing	Remove
□	qadevvm9.sensage.com		Installing	Remove

Choose Services

1 In the Choose Services screen (shown below) choose the services. By default, the three services that you must install are chosen for you.



Choose Services

Choose which services you want to install on your cluster.

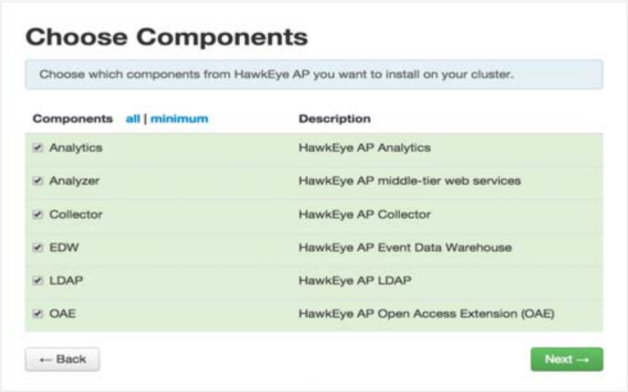
Service all | minimum	Version	Description
☑ Nagios	3.2.3	Nagios Monitoring and Alerting system
☑ Ganglia	3.2.0	Ganglia Metrics Collection system
☑ HawkEye AP	6.0.1	The Data Analytics Platform

2 Click **Next**.

Choose Components

1 In the Choose Components screen (shown below) choose the components that you want to install on your HawkEye AP cluster. For details on these components, see “HawkEye AP Overview”, on page 13. Select all to preselect all items or minimum to preselect from these choices: Analyzer, OAE, EDW LAPD, EDW, and Collector.

NOTE: Use the check boxes to check off any product you want to install; you can select whatever you like; the system will select the dependent components automatically. if the component has any dependencies that must be selected.



Choose Components

Choose which components from HawkEye AP you want to install on your cluster.

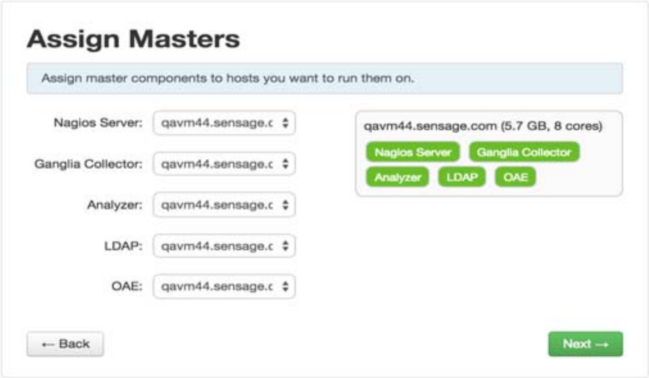
Components all | minimum	Description
☑ Analytics	HawkEye AP Analytics
☑ Analyzer	HawkEye AP middle-tier web services
☑ Collector	HawkEye AP Collector
☑ EDW	HawkEye AP Event Data Warehouse
☑ LDAP	HawkEye AP LDAP
☑ OAE	HawkEye AP Open Access Extension (OAE)

2 When you have finished your selection(s), click **Next**.

Assign Masters

1 In the Assign Masters screen (shown below) assign the master components to the hosts that you want to run them on. Click the UP and DOWN arrow in the list box to make your host selection for each component.

NOTE: By default, Master Services are selected on one host. You can click the dropdown list box under each component to change the host(s) assignment.



Assign Masters

Assign master components to hosts you want to run them on.

Nagios Server: qavm44.sensage.c

Ganglia Collector: qavm44.sensage.c

Analyzer: qavm44.sensage.c

LDAP: qavm44.sensage.c

OAE: qavm44.sensage.c

qavm44.sensage.com (5.7 GB, 8 cores)

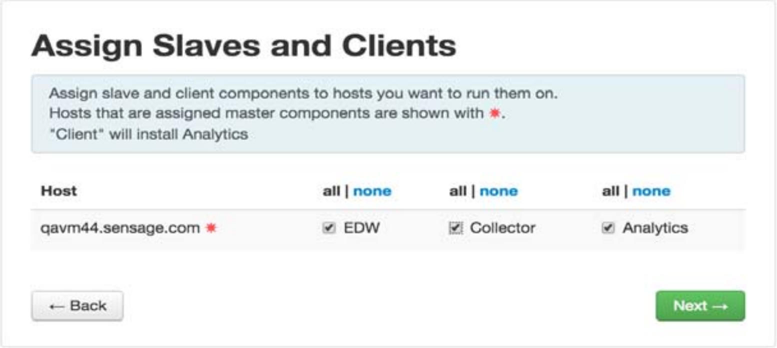
2 When you have finished your selection(s), click **Next**.

Assign Slaves and Clients

1 In the Assign Slaves and Clients screen (shown below) assign the slave and client components to the hosts that you want to run them on. Note that the host that is the master and that has been assigned master components from the previous screen is identified with an * (asterisk).

Use the check boxes to make your slave and client component selection. You may also select all or none to select an entire column of the same component or select none to deselect the entire column. You can install more than one component on one host.

IMPORTANT: You need to make sure you have assigned a component to one of the hosts or will get an error message that you need to select at least one host for one component. You can have slave components on the master host.



Assign Slaves and Clients

Assign slave and client components to hosts you want to run them on.
Hosts that are assigned master components are shown with ✱.
"Client" will install Analytics

Host	all | none	all | none	all | none
qavm44.sensage.com ✱	☑ EDW	☑ Collector	☑ Analytics

2 When you have finished your selection(s), click **Next**.

Customize Services

1 In the Customize Services screen (shown below) you are presented with a set of tabs that let you manage configuration settings for HawkEye AP components. The number beside a tab indicates how many parameters you are required to set. For all other parameters, the wizard sets defaults for each setting, which you must not change.

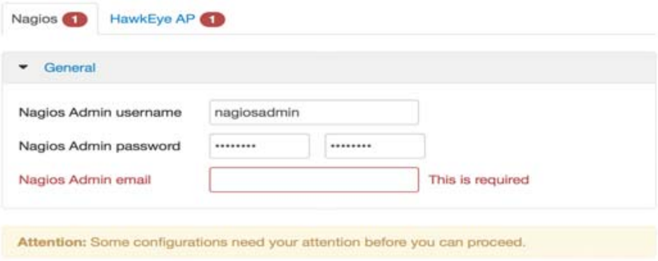
Hover your mouse over each of the properties to see a brief description of what it does. The number of tabs you see is based on the type of installation you have decided to do.

Following are the required entries for each tab. You click the appropriate tab to expand and collapse the display.

Nagios Tab

a To create your Nagios Admin username and password, enter both on the lines specified (as shown below) and confirm your entry. The default password for the nagiosadmin user is **changeme**.

b Enter the Nagios Admin email address.



Nagios Admin username: nagiosadmin

Nagios Admin password: •••••••• ••••••••

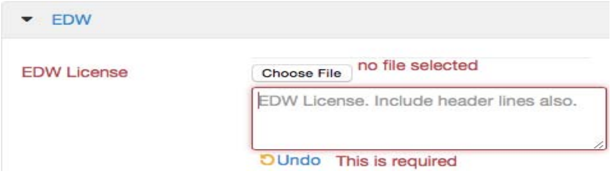
Nagios Admin email: This is required

Attention: Some configurations need your attention before you can proceed.

HawkEye AP Tab

1 Click the HawkEye AP tab. In this tab you are only required to set one parameter where you must provide your EDW License key. Optionally, you may configure additional EDW instances using the EDW Ports field (see Step 2).

As shown in the screen example, click **Choose File** to populate the license file from a specific location. The file that you choose must be in UNIX format.



EDW

EDW License

no file selected

EDW License. Include header lines also.

This is required

2 In the EDW Ports field, enter a comma-separated list of port numbers, providing one port for each EDW instance that you want to create. For example, to configure two instances, enter a list of two port numbers.

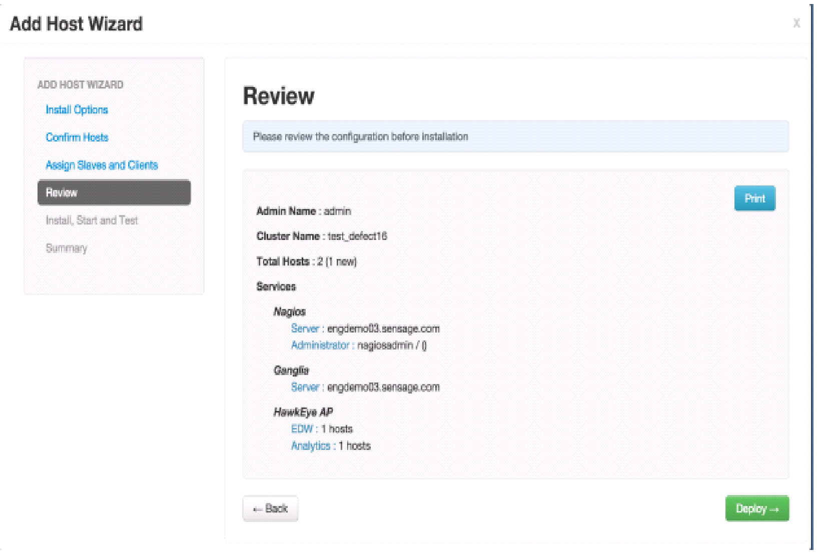
NOTE: Running multiple EDW instances on each server improves utilization of servers with a large number of cores and a large amount of memory.

The number of EDW instances on each server is the same within a HawkEye AP cluster. You do not have the option to set a different number of EDW instances on different servers in the same HawkEye AP cluster.

3 Click **Next** and review what has been configured. You cannot change the port list (by reconfiguring EDW) after the installation completes.

Review your Installation

When your configuration settings are applied, you will see a Review screen displayed, similar to the one below. The display will tell you what component was installed on each host of your cluster. You may click print to obtain a print out.



Add Host Wizard

Review

Please review the configuration before installation

Admin Name : admin

Cluster Name : test_defect16

Total Hosts : 2 (1 new)

Services

Nagios
Server : engdemo03.sensage.com
Administrator : nagiosadmin / ()

Ganglia
Server : engdemo03.sensage.com

HawkEye AP
EDW : 1 hosts
Analytics : 1 hosts

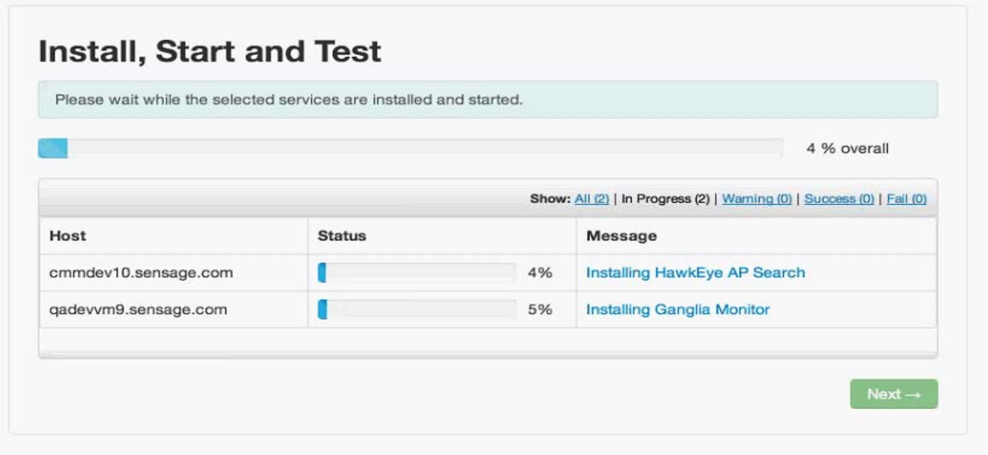
If the installation is accurate, you can proceed with installation and deployment. However, If you detect any issues with the review, then you will need to select Back button until you return to the applicable screen to make your necessary changes or click on the links to the screen provided on the left page to navigate back to the desired page.

After you have confirmed the configuration settings, click **Deploy** which will install the product.

Install, Start, and Test HawkEye AP

The Install, Start, and Test screen (shown below) provides the progress of the install. It will take approximately 10 to 15 minutes to complete.

After the component is started, a simple test is run on it. The screen provides an overall progress of the status and a host- by-host status in the main section.



Install, Start and Test

Please wait while the selected services are installed and started.

4 % overall

Show: All (2) | In Progress (2) | Warning (0) | Success (0) | Fail (0)

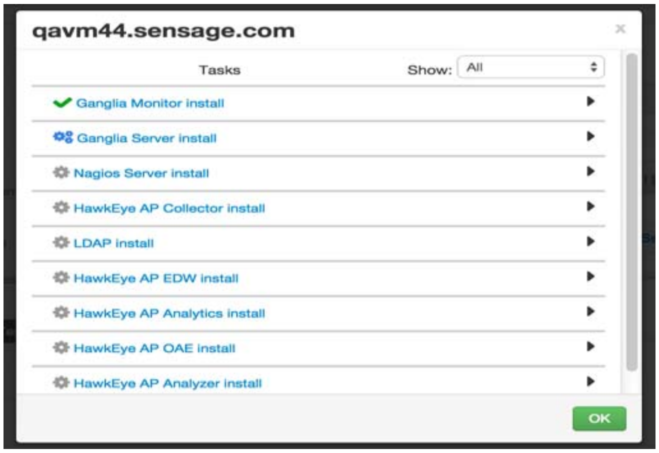
Host	Status	Message
cmmdev10.sensage.com	4%	Installing HawkEye AP Search
qadevvm9.sensage.com	5%	Installing Ganglia Monitor

To view specific information on what tasks have been completed per host, click the link in the Message column for the appropriate host. The log files themselves are contained in the Ambari server at:

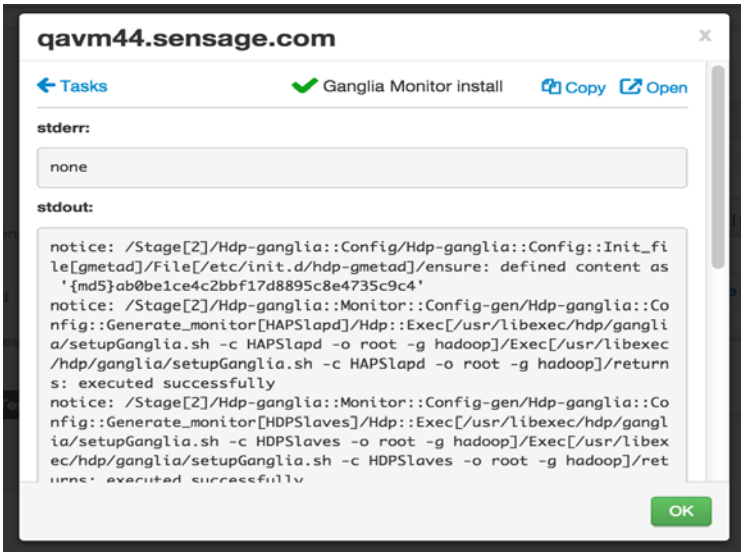
```
$ cd /var/log/ambari-server/
```

To view any specific status messages that may appear during the installation, click the applicable link on the upper right side of the screen, which will indicate the number of messages beside its type; for example **Warning (2)**.

Below is a sample of the information that is provided when you click the Message text for the status of a specific host. In the sample below, cmmedev10.sensage.com was selected and all components and their (status) represented by the icon are displayed. Currently HawkEye AP Search install is now in progress.



If you click an individual task under **Tasks**, you will see more details on the component's progress through the related **stderr** and **stdout** output (as shown below). Click **OK** to return to the Install, Start, and Test screen.



stderr:

```
none
```

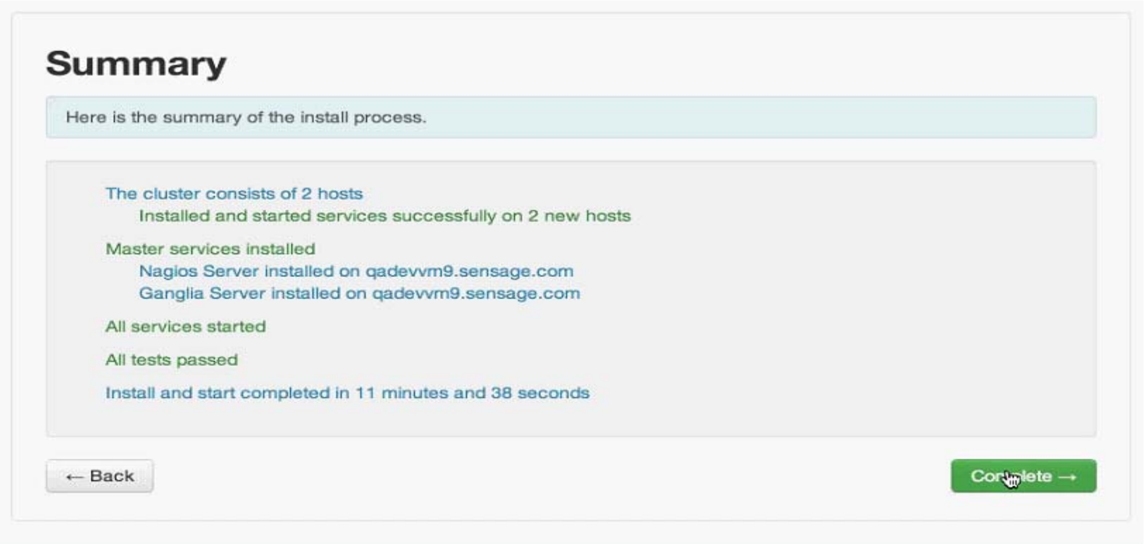
stdout:

```
notice: /Stage[2]/Hdp-ganglia::Config/Hdp-ganglia::Config::Init_fi
le[gmetad]/File[/etc/init.d/hdp-gmetad]/ensure: defined content as
 '{md5}ab0be1ce4c2bbf17d8895c8e4735c9c4'
notice: /Stage[2]/Hdp-ganglia::Monitor::Config-gen/Hdp-ganglia::Co
nfig::Generate_monitor[HAPSlapd]/Hdp::Exec[/usr/libexec/hdp/gangli
a/setupGanglia.sh -c HAPSlapd -o root -g hadoop]/Exec[/usr/libexec
/hdp/ganglia/setupGanglia.sh -c HAPSlapd -o root -g hadoop]/return
s: executed successfully
notice: /Stage[2]/Hdp-ganglia::Monitor::Config-gen/Hdp-ganglia::Co
nfig::Generate_monitor[HDPSlaves]/Hdp::Exec[/usr/libexec/hdp/gangl
ia/setupGanglia.sh -c HDPSlaves -o root -g hadoop]/Exec[/usr/libex
ec/hdp/ganglia/setupGanglia.sh -c HDPSlaves -o root -g hadoop]/ret
urns: executed successfully
```

After successful completion, click **Next**, which will display a summary page to review what you have installed.

View Summary

When the install is completed, the Summary page (shown below) gives you a summary of the accomplished tasks.



Summary

Here is the summary of the install process.

The cluster consists of 2 hosts
    Installed and started services successfully on 2 new hosts

Master services installed
    Nagios Server installed on qadevvm9.sensage.com
    Ganglia Server installed on qadevvm9.sensage.com

All services started

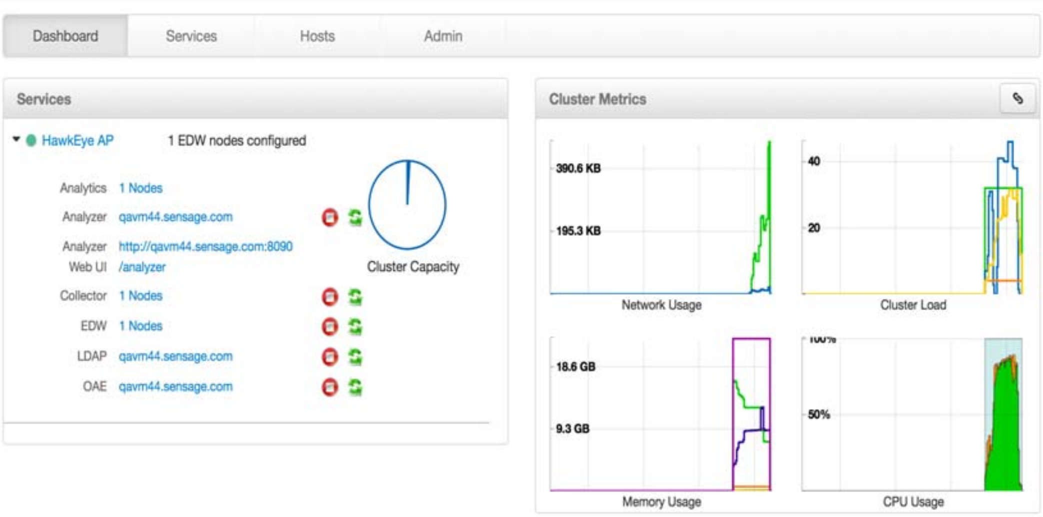
All tests passed

Install and start completed in 11 minutes and 38 seconds

Click **Complete**.

VERIFY YOUR INSTALLATION

After you have clicked **Complete**, the HawkEye AP Management page (example shown below) provides you with detailed information about your deployment. All of your components should be in operation. From this page you can perform such tasks as starting and stopping components, viewing what services are not running, adding another user to the system, another host to the cluster, or another component. For more details, see the *Administration Guide*.



Services

▾ ● HawkEye AP   1 EDW nodes configured

Analytics	1 Nodes
Analyzer	qavm44.sensage.com
Analyzer Web UI	http://qavm44.sensage.com:8090 /analyzer
Collector	1 Nodes
EDW	1 Nodes
LDAP	qavm44.sensage.com
OAE	qavm44.sensage.com

PERFORM POST-INSTALLATION TASKS

The following tasks may be completed after the installation:

- “Getting the latest OAE Schema Updates from EDW”, next
- “Enabling Log Adapters”, on page 54
- “Removing the Distribution File”, on page 54
- “Starting Ganglia after Installation”, on page 55
- “Optional: Installing HawkEye AP with the Deployment Manager Tool”, on page 56

Getting the latest OAE Schema Updates from EDW

To obtain the latest updates to the EDW database without recreating the entire OAE external schema, use:

Run the following command on the Analyzer host:

```
/opt/hexis/hawkeye-ap/bin/psql -U <PG_USER> -d controller -c “SELECT
oae.force_sync(‘<EDW_INSTANCE_NAME>’);”
```

Example:

```
/opt/hexis/hawkeye-ap/bin/psql –U hexis -d controller -c “SELECT
oae.force_sync(‘default’);”
```

Enabling Log Adapters

After you successfully install HawkEye AP on the hosts in your deployment, you must enable each of the log adapters you want to use with the collectorAdmin command as shown below. Note that you can use the same command to disable any log adapters you have enabled.

```
/opt/hexis/hawkeye-ap /bin/collectorAdmin enable | disable <adapter_name>
```

The following example assumes you want to enable the Unix sshd2 log adapter:

```
/opt/hexis/hawkeye-ap/bin/collectorAdmin enable unix_sshd2_syslogng
```

You can enable or disable more than one adapter at a time. For example:

```
/opt/hexis/hawkeye-ap/bin/collectorAdmin enable unix_sudo_syslogng enable
unix_ftpd_syslogng
```

Removing the Distribution File

After you successfully install HawkEye AP on the hosts in your deployment, you can remove the distribution tar file that you downloaded from the HawkEye AP Support Web site.

To remove the distribution file

1 Switch to the root user:

```
su -
```

2 Change to the directory into which you downloaded the distribution file. This is the same directory that contains the staging directory on the central installation host; for example:

```
cd /tmp
```

3 Remove the file:

```
rm -f hawkeye-ap-<release_specific_information>.tar.gz
```

Starting Ganglia after Installation

Ganglia can go down intermittently after a fresh installation, especially on large clusters (96 nodes). If this is the case, since Ganglia cannot be started from the GUI, perform the following workaround to start from the command line first and then from the GUI:

1 Go the host where you have ganglia-server installed.

2 Run service Ganglia start.

3 Return to Ambari UI.

4 Start Ganglia service.

Optional: Installing HawkEye AP with the Deployment Manager Tool

As an alternative to installing HawkEye AP via the Deployment Manager web interface described in the previous section, you can use a command line tool called hawkeye-deploy. Note that the web interface should be the preferred choice because it is more user-friendly and optimized to complete the installation more quickly and efficiently.

To install HawkEye AP with hawkeye-deploy, perform the following steps:

1. After running the `install.sh` script, install lms-ambari-client on the Deployment by issuing the following command:

   ```
   yum install lms-ambari-client
   ```

2. Install Ganglia by issuing the following commands:

   ```
   hawkeye-deploy -k <ssh key file> --cluster=<cluster_name> --
   targetComponent=gangliaServer --action=install --
   gangliaHost=<ganglia_server_host>
   hawkeye-deploy --cluster=<cluster_name> --targetComponent=gangliaServer --
   action=start
   ```

3. Install Nagios by issuing the following commands:

   ```
   hawkeye-deploy -k <ssh key file> --cluster=<cluster_name> --
   targetComponent=nagiosServer --action=install --
   nagiosHost=<nagios_server_host> --adminEmail=<admin email>
   hawkeye-deploy --cluster=<cluster_name> --targetComponent=nagiosServer --
   action=start
   ```

4. Install LDAP by issuing the following commands:

   ```
   hawkeye-deploy -k <ssh key file> --cluster=<cluster_name> --
   ldapHost=<sensage_ldap_host> --targetComponent=ldap --action=install
   hawkeye-deploy --cluster=<cluster_name> --targetComponent=ldap --action=start
   ```

   Optional Install Parameters:

   - **--ldapPass=**<ldap password>
   - **--ldapPort=**<ldap port>
   - **--ldapDomain=**<ldap domain>

5. Install EDW by issuing the following commands:

   ```
   hawkeye-deploy -k <ssh key file> --cluster=<cluster_name> --
   ldapHost=<sensage_ldap_host> --licenseFile=<path to sls license file> --
   edwHosts=<sensage_sls_host> --targetComponent=edw --action=install
   hawkeye-deploy --cluster=<cluster_name> --targetComponent=edw --action=start
   ```

   Optional Install Parameters:

   - **--edwPorts=**<comma-separated list of EDW ports>

- **--instance=**< instance name>
- **--licenseFile**=<Path to License File>
- **--edwAdminPass=**<EDW Admin password>
- **--edwGuestPass=**<EDW Guest password>
- **--edwSysPass=**<EDW System password>
- **--edwOaePass=**<EDW OAE password>
- **--edwDataDir=**<EDW Data Directory>

6 Install OAE by issuing the following commands:

```
hawkeye-deploy -k <ssh key file> --cluster=<cluster_name> --
targetComponent=oae --action=install --oaeHost=<oae host>
hawkeye-deploy --cluster=<cluster_name> --targetComponent=oae --action=start
```

Optional Install Parameters:

- **--oaeDataDir=**<OAE Data Directory>

7 Install Analyzer by issuing the following commands:

```
hawkeye-deploy -k <ssh key file> --cluster=<cluster_name> --
targetComponent=analyzer --action=install
hawkeye-deploy --cluster=<cluster_name> --targetComponent=analyzer --
action=start
```

8 Install Collector by issuing the following commands:

```
hawkeye-deploy -k <ssh key file> --cluster=<cluster_name> --
collectorHosts=<sensage_collector_hosts> --targetComponent=collector --
action=install
```

Optional Install Parameters:

- **--collectorHead=**<Collector hosts head>

9 Install Analytics by issuing the following commands:

```
hawkeye-deploy --cluster=<cluster_name> --targetComponent=analytics --
action=install
```

CHAPTER 4

Extending the Event Data Warehouse (EDW)

After you install HawkEye AP, you can extend the EDW with the procedure in this chapter.

IMPORTANT: Use of Nearline Storage

When extending the EDW cluster with data archived to a nearline storage such as centera, you must copy the pea and nsllist files to an extended node to ensure successful completion of the EDW extension. To do this:

1 Copy the **nsilist.dat** file from the existing EDW node to the extended node and make sure it is owned by the Hexis user.

2 Copy the pea file from the existing EDW node to the extended EDW node. You can find its location from nsilist.dat file (everything after the '**?**'):

For example:

```
testNSI centera://168.159.214.20?/local/c1profile3.pea
```

3 Restart nss/edw on the extended node.

EDW Extension Procedure

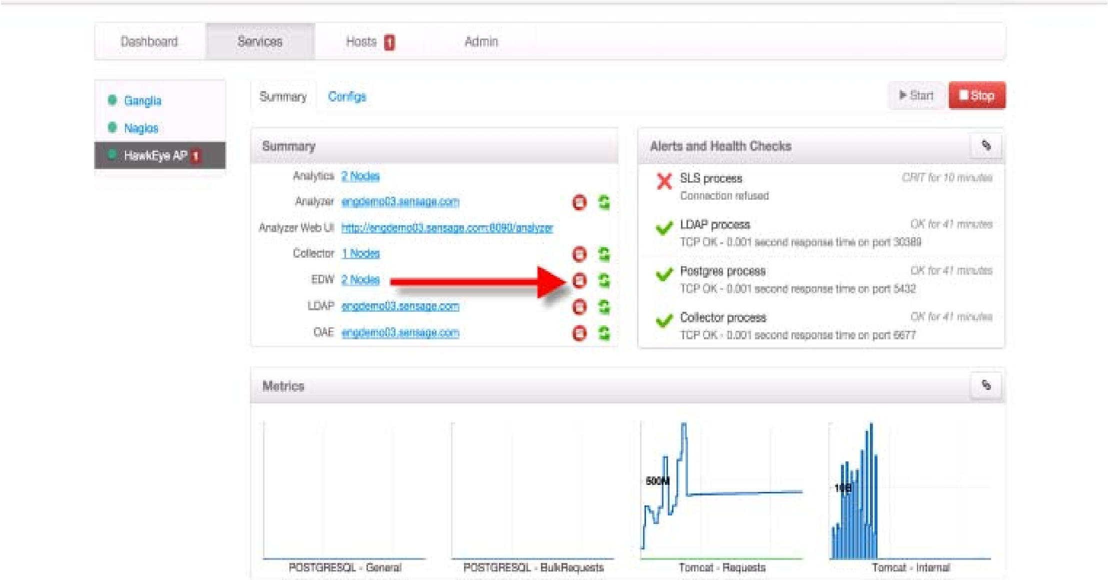
1 If your system has been upgraded from HawkEye AP 5.x.x, you are required to set some variables in the Ambari server prior to attempting EDW extension.

Issue the following commands running as root on the Deployment Manager:

```
echo -n "<?xml version='1.0' encoding='utf-
8'?><ambari><ambari_server_priv_key>" > /tmp/pk.xml
cat /root/.ssh/id_dsa >> /tmp/pk.xml
echo "</ambari_server_priv_key><ambari_cluster_name>mycluster</
ambari_cluster_name><ambari_server>myserver:8443</ambari_server></ambari>" >>
/tmp/pk.xml
hawkeye-deploy --targetService=hawkeyeAP --action=reconfigure --configFile=/
tmp/pk.xml
rm -f /tmp/pk.xml
```

NOTE: Substitute your Ambari cluster name for "mycluster" and your Deployment Manager fully qualified host name for "myserver".

1 Login to Deployment Manager UI and stop the EDW service. To do this, click the "red circle" next to the EDW in the Summary tab.



Summary

Analytics	2 Nodes
Analyzer	engdemo03.sensage.com
Analyzer Web UI	http://engdemo03.sensage.com:8080/analyzer
Collector	1 Nodes
EDW	2 Nodes
LDAP	engdemo03.sensage.com
OAE	engdemo03.sensage.com

Alerts and Health Checks

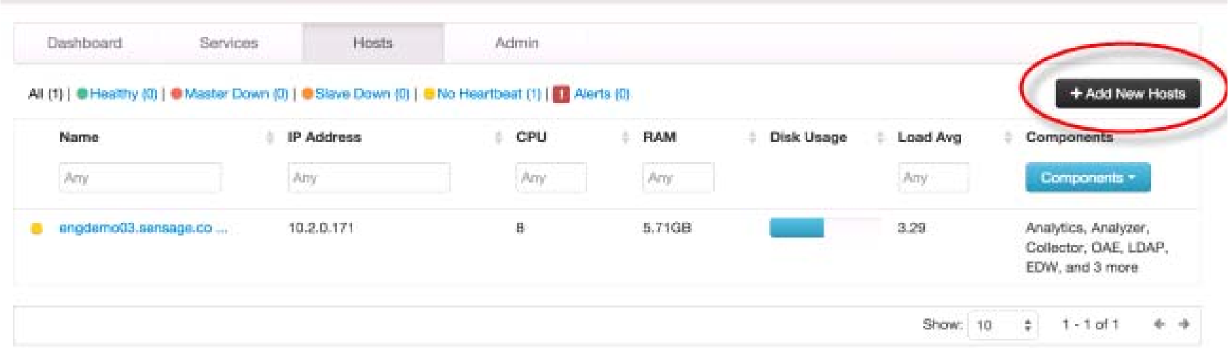
✗ SLS process — CRIT for 10 minutes
Connection refused

✓ LDAP process — OK for 41 minutes
TCP OK - 0.001 second response time on port 30389

✓ Postgres process — OK for 41 minutes
TCP OK - 0.001 second response time on port 5432

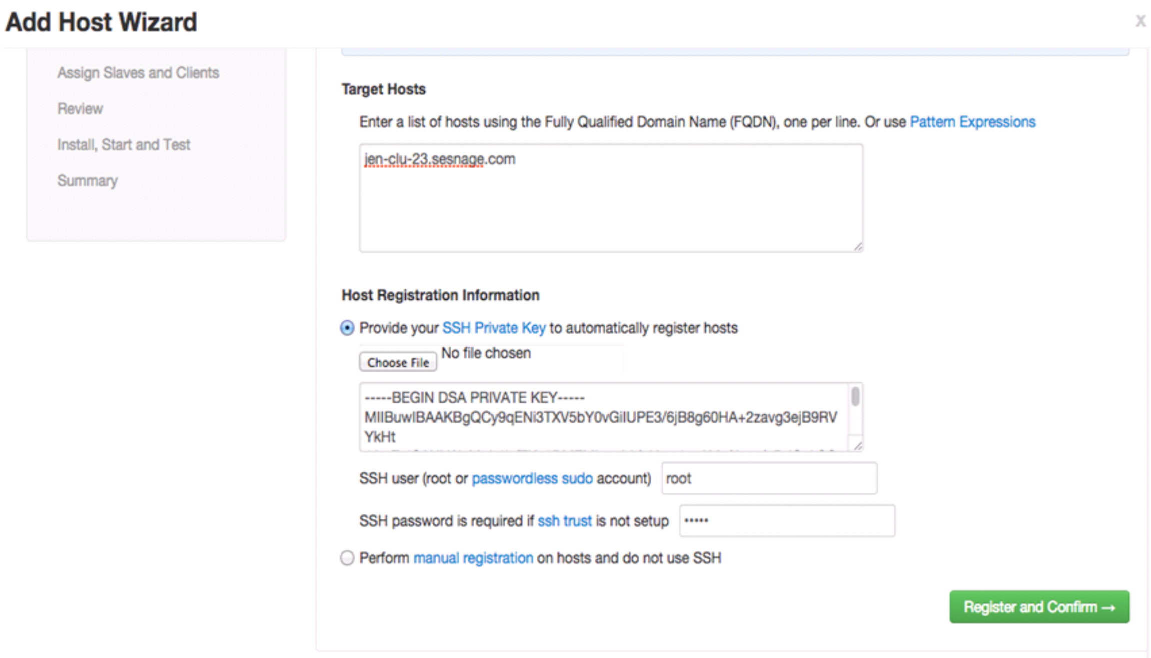
✓ Collector process — OK for 41 minutes
TCP OK - 0.001 second response time on port 5677

2 From the Deployment Manager UI, click **+ Add New Hosts** button in the Hosts tab.


Dashboard
Services
Hosts
Admin
All (1) | ● Healthy (0) | ● Master Down (0) | ● Slave Down (0) | ● No Heartbeat (1) | ! Alerts (0)
+ Add New Hosts
Components ▾
Show: 10
1 - 1 of 1

	Name	IP Address	CPU	RAM	Disk Usage	Load Avg	Components
	Any	Any	Any	Any		Any	Components ▾
●	engdemo03.sensage.co ...	10.2.0.171	8	5.71GB		3.29	Analytics, Analyzer, Collector, OAE, LDAP, EDW, and 3 more

3 Enter the target host(s) on which you are deploying the product as shown in the screen example below.



Add Host Wizard

Target Hosts

Enter a list of hosts using the Fully Qualified Domain Name (FQDN), one per line. Or use Pattern Expressions

jen-clu-23.sesnage.com

Host Registration Information

● Provide your SSH Private Key to automatically register hosts

Choose File No file chosen

```
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQCy9qENi3TXV5bY0vGiIUPE3/6jB8g60HA+2zavg3ejB9RV
YkHt
```

SSH user (root or passwordless sudo account) root

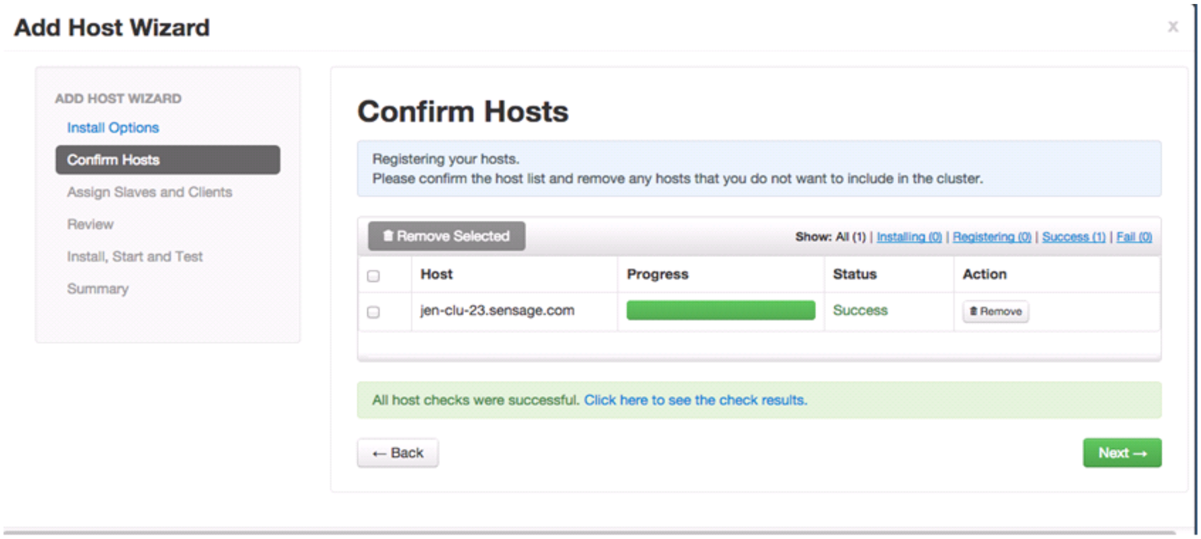
SSH password is required if ssh trust is not setup •••••

○ Perform manual registration on hosts and do not use SSH

NOTE: If you use a pattern expression to provide the hosts, the system displays a popup with an expanded list of host(s).

4 Click the **Register and Confirm** button.

5 In the Confirm Hosts screen (shown below), confirm that HawkEye AP has located the correct hosts for your cluster and at the end of the list, click to check results.



Add Host Wizard

Confirm Hosts

Registering your hosts.
Please confirm the host list and remove any hosts that you do not want to include in the cluster.

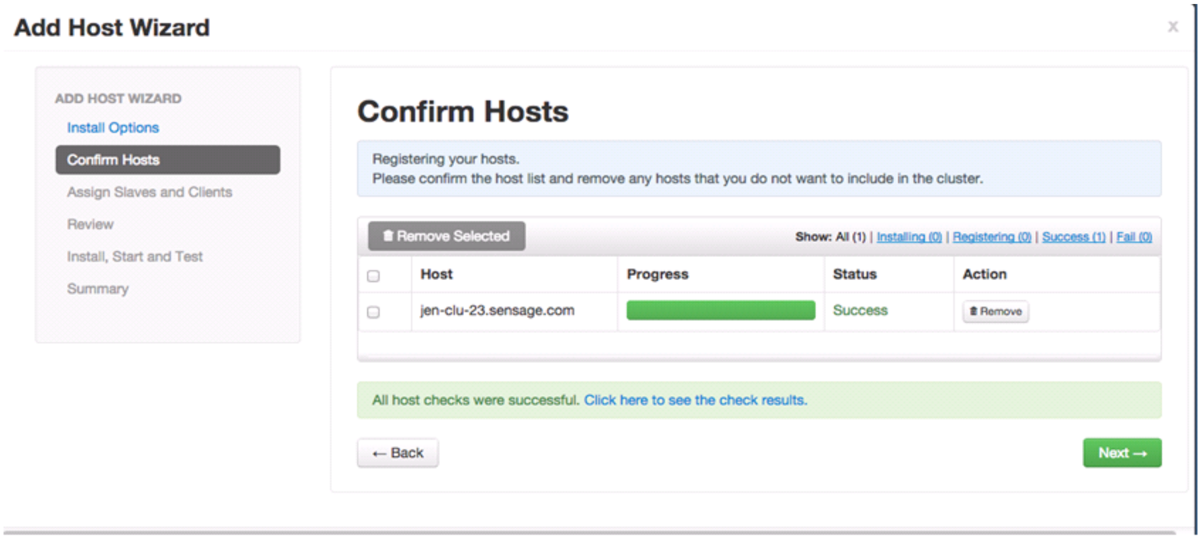
Show: All (1) | Installing (0) | Registering (0) | Success (1) | Fail (0)

□	Host	Progress	Status	Action
□	jen-clu-23.sensage.com	🟩	Success	Remove

All host checks were successful. Click here to see the check results.

NOTE: You can remove any host by selecting the appropriate check boxes and clicking the grey **Remove Selected** button. To remove a single host, click **Remove** in the Action column.

During the check process, a yellow box indicates some warnings that were encountered during the check process. Click to see a list of what was checked and what caused the warning.



Confirm Hosts

Registering your hosts.
Please confirm the host list and remove any hosts that you do not want to include in the cluster.

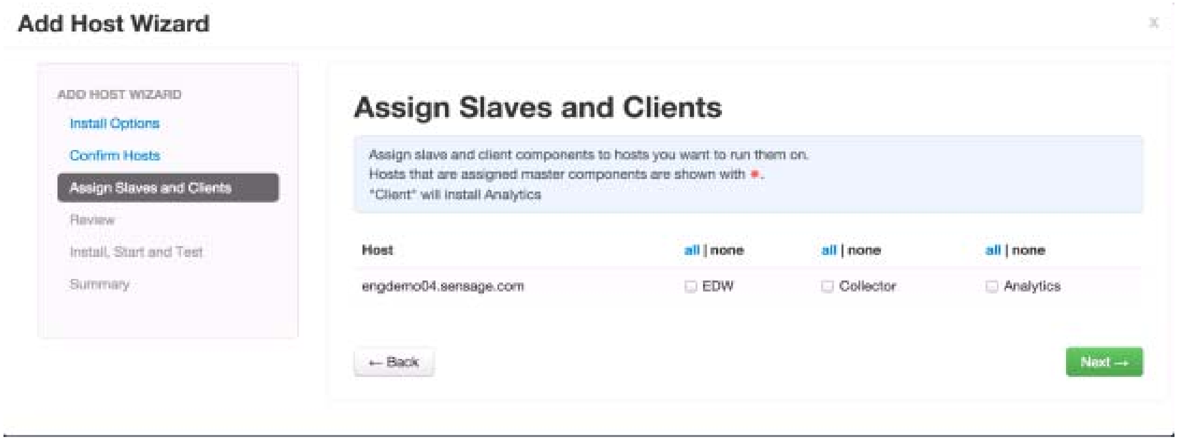
□	Host	Progress	Status	Action
□	jen-clu-23.sensage.com	🟩	Success	Remove

All host checks were successful. Click here to see the check results.

When you are satisfied with the list of hosts, click **Next** on successful registration.

6 Select EDW in the "Assign Slaves and Clients" window (by default, all is selected under each Host component). Unselect Collector.

NOTE: On selecting EDW, Analytics will be selected automatically.



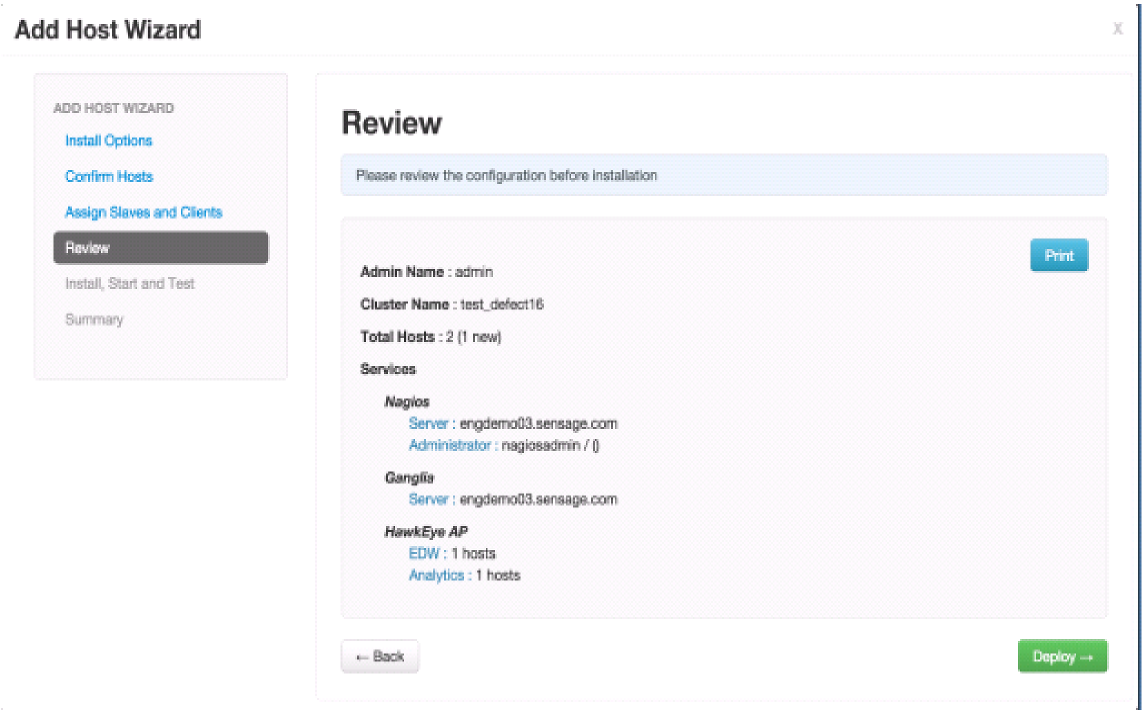
Assign Slaves and Clients

Assign slave and client components to hosts you want to run them on.
Hosts that are assigned master components are shown with ✱.
"Client" will install Analytics

Host	all | none	all | none	all | none
engdemo04.sensage.com	□ EDW	□ Collector	□ Analytics

7 When you have finished your selection(s), click **Next**.

8 After you have confirmed the configuration setting, click **Deploy** which will install the product.



Review

Please review the configuration before installation

Admin Name : admin

Cluster Name : test_defect16

Total Hosts : 2 (1 new)

Services

Nagios
Server : engdemo03.sensage.com
Administrator : nagiosadmin / ()

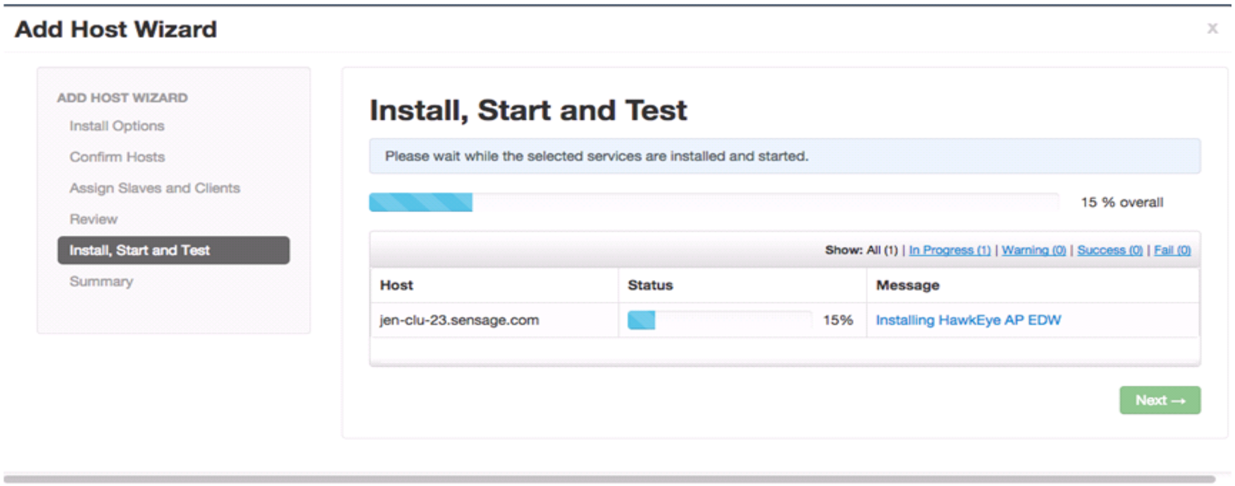
Ganglia
Server : engdemo03.sensage.com

HawkEye AP
EDW : 1 hosts
Analytics : 1 hosts

9 Install, Start and Test:

The Install, Start, and Test screen (shown below) provides the progress of the install. It will take approximately 10 to 15 minutes to complete.

The screen provides an overall progress of the status and a host-by-host status in the main section (as shown below).



Install, Start and Test

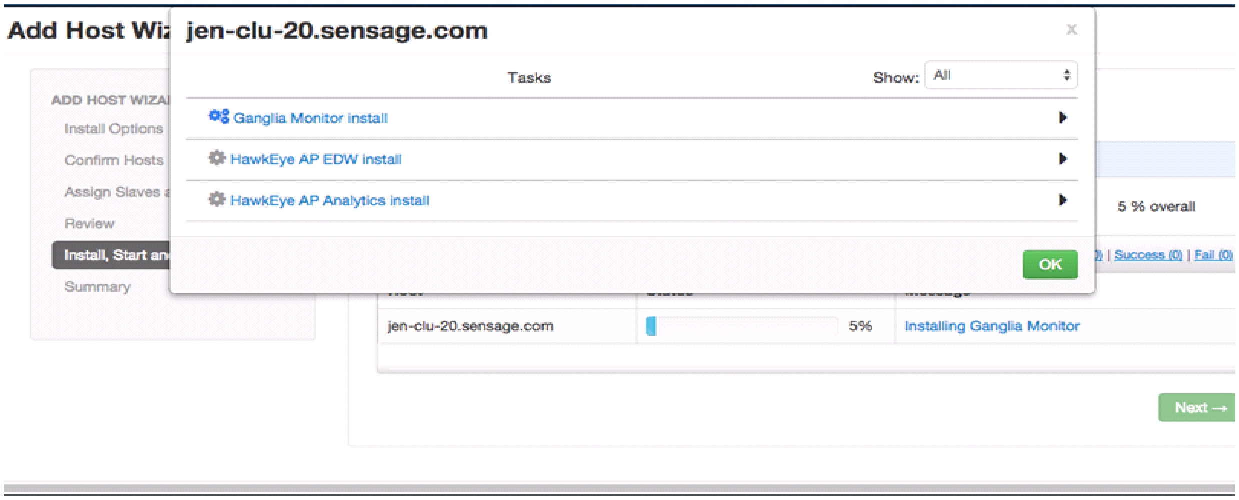
Please wait while the selected services are installed and started.

15 % overall

Show: All (1) | In Progress (1) | Warning (0) | Success (0) | Fail (0)

Host	Status	Message
jen-clu-23.sensage.com	15%	Installing HawkEye AP EDW

Below is a sample of the information that is provided when you click the Message text for the status of a specific host:

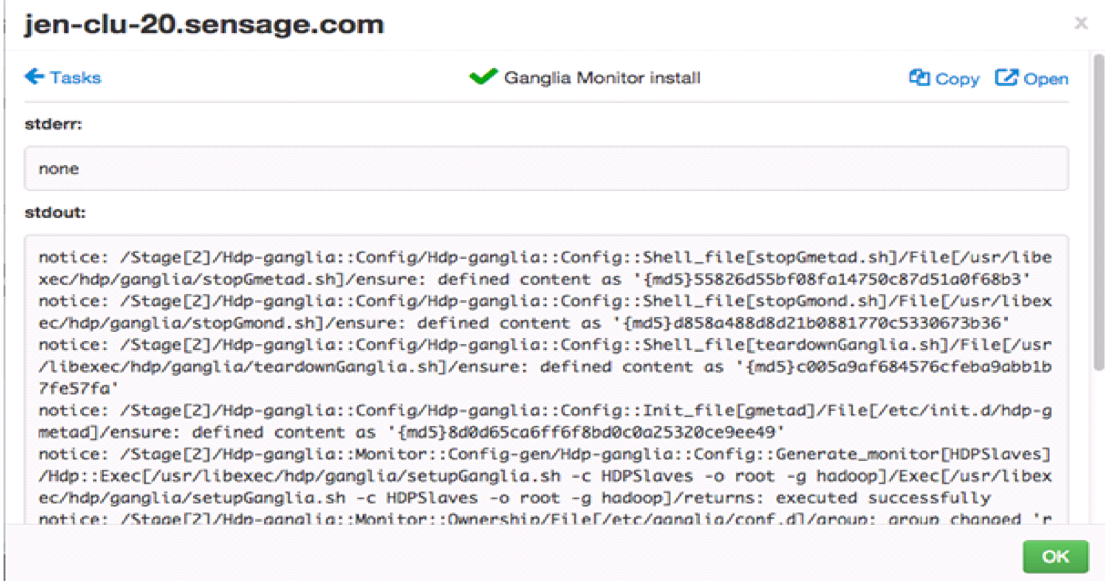


jen-clu-20.sensage.com

Tasks	Show: All
Ganglia Monitor install	
HawkEye AP EDW install	
HawkEye AP Analytics install	

jen-clu-20.sensage.com	5%	Installing Ganglia Monitor

10 If you click an individual task under Tasks, you will see more details on the component's progress through the related stderr and stdout output (as shown below). Click **OK** to return to the Install, Start, and Test screen.



jen-clu-20.sensage.com

✓ Ganglia Monitor install

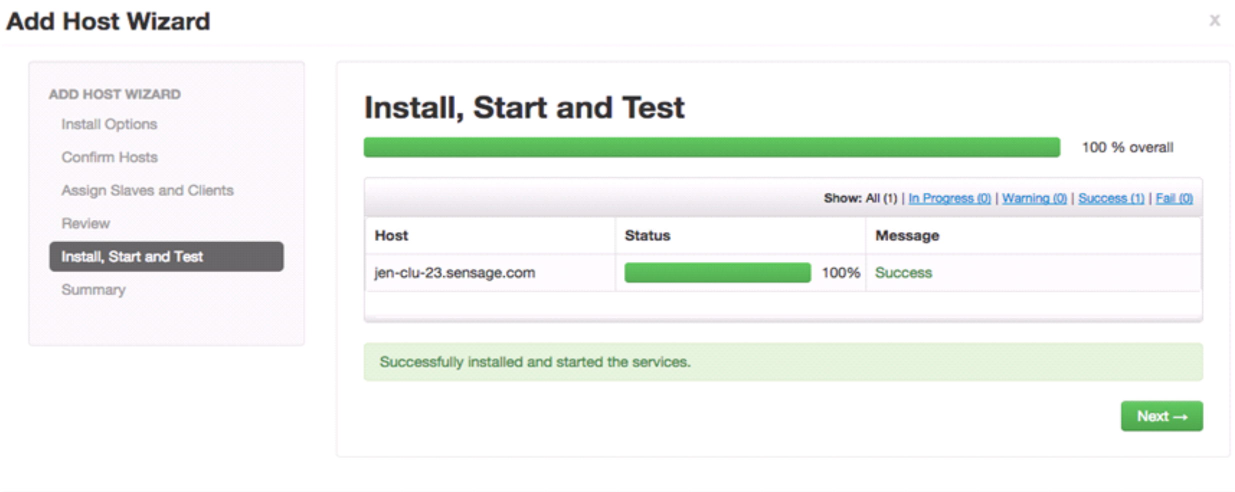
stderr:

```
none
```

stdout:

```
notice: /Stage[2]/Hdp-ganglia::Config/Hdp-ganglia::Config::Shell_file[stopGmetad.sh]/File[/usr/libe
xec/hdp/ganglia/stopGmetad.sh]/ensure: defined content as '{md5}55826d55bf08fa14750c87d51a0f68b3'
notice: /Stage[2]/Hdp-ganglia::Config/Hdp-ganglia::Config::Shell_file[stopGmond.sh]/File[/usr/libex
ec/hdp/ganglia/stopGmond.sh]/ensure: defined content as '{md5}d858a488d8d21b0881770c5330673b36'
notice: /Stage[2]/Hdp-ganglia::Config/Hdp-ganglia::Config::Shell_file[teardownGanglia.sh]/File[/usr
/libexec/hdp/ganglia/teardownGanglia.sh]/ensure: defined content as '{md5}c005a9af684576cfeba9abb1b
7fe57fa'
notice: /Stage[2]/Hdp-ganglia::Config/Hdp-ganglia::Config::Init_file[gmetad]/File[/etc/init.d/hdp-g
metad]/ensure: defined content as '{md5}8d0d65ca6ff6f8bd0c0a25320ce9ee49'
notice: /Stage[2]/Hdp-ganglia::Monitor::Config-gen/Hdp-ganglia::Config::Generate_monitor[HDPSlaves]
/Hdp::Exec[/usr/libexec/hdp/ganglia/setupGanglia.sh -c HDPSlaves -o root -g hadoop]/Exec[/usr/libex
ec/hdp/ganglia/setupGanglia.sh -c HDPSlaves -o root -g hadoop]/returns: executed successfully
notice: /Stage[2]/Hdp-ganglia::Monitor::Ownership/File[/etc/ganglia/conf.d]/group: group changed 'r
```

11 After successful completion, click Next, which will display a summary page to review what you have installed.

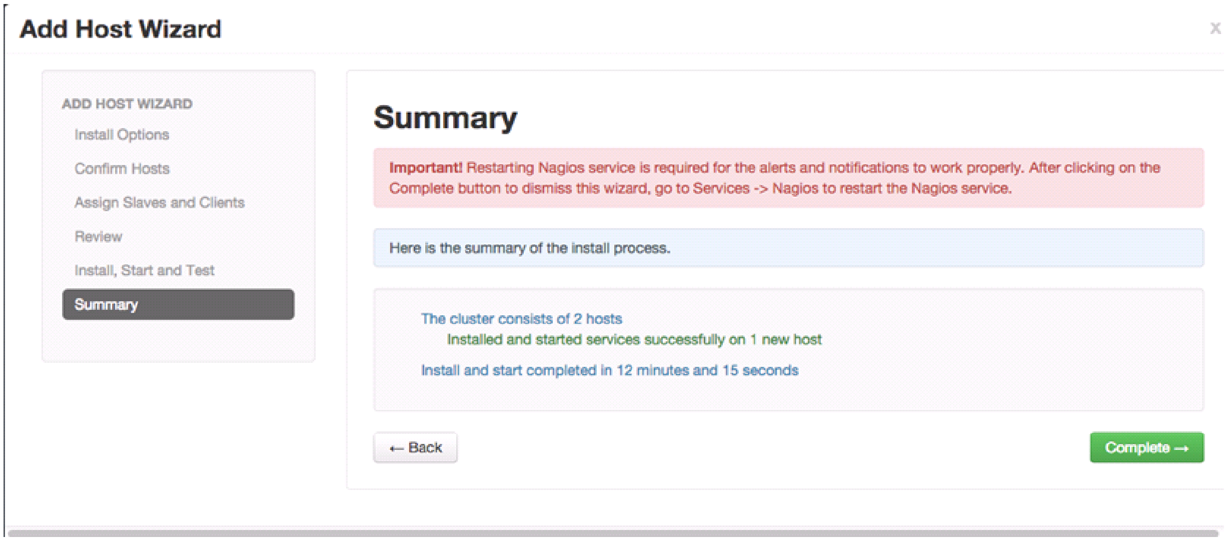


Host	Status	Message
jen-clu-23.sensage.com	100%	Success

Successfully installed and started the services.

12 View Summary:

When the install is completed, the Summary page (shown below) gives you a summary of the accomplished tasks.



Important! Restarting Nagios service is required for the alerts and notifications to work properly. After clicking on the Complete button to dismiss this wizard, go to Services -> Nagios to restart the Nagios service.

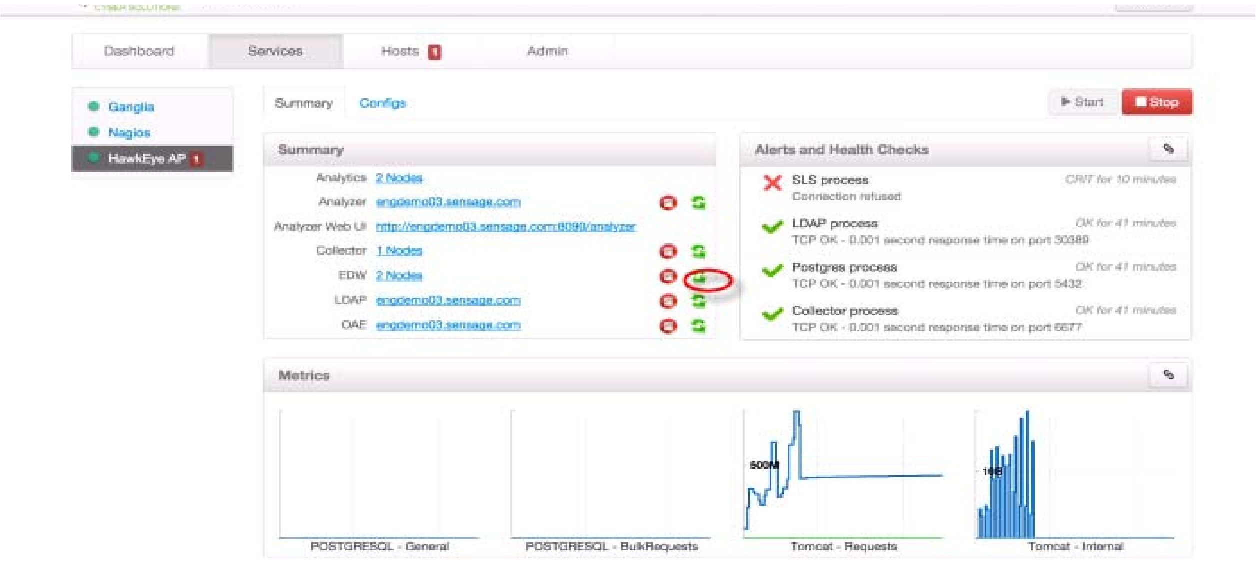
Here is the summary of the install process.

The cluster consists of 2 hosts
Installed and started services successfully on 1 new host

Install and start completed in 12 minutes and 15 seconds

IMPORTANT: Restarting Nagios service is required for the alerts and notifications to work properly. After clicking the **Complete** button to dismiss the wizard, go to **Service -> Nagios** to restart the Nagios service.

13 Navigate to Service tab and click **Restart** button next to EDW to restart the EDW on all hosts.



Summary

Analytics 2 Nodes
Analyzer engdemo03.sensage.com
Analyzer Web UI http://engdemo03.sensage.com:8090/analyzer
Collector 1 Nodes
EDW 2 Nodes
LDAP engdemo03.sensage.com
OAE engdemo03.sensage.com

Alerts and Health Checks

SLS process — CRIT for 10 minutes
Connection refused

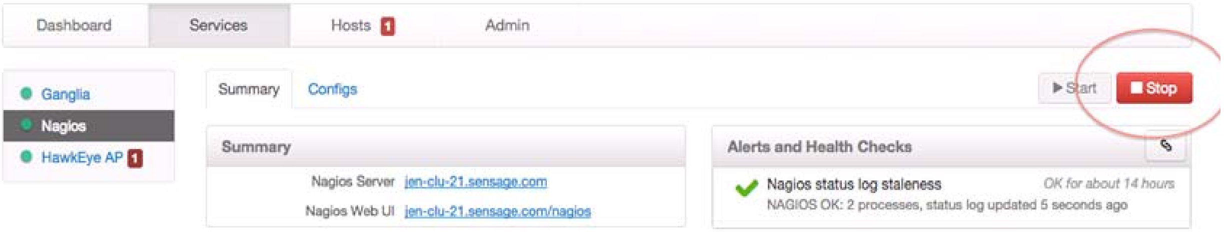
LDAP process — OK for 41 minutes
TCP OK - 0.001 second response time on port 30389

Postgres process — OK for 41 minutes
TCP OK - 0.001 second response time on port 5432

Collector process — OK for 41 minutes
TCP OK - 0.001 second response time on port 6677

14 Start/stop Nagios service:

Restarting Nagios service is required for the alerts and notifications to work properly. Navigate to services/NAGIOS/summary and click the **Stop** button to stop Nagios.



Summary

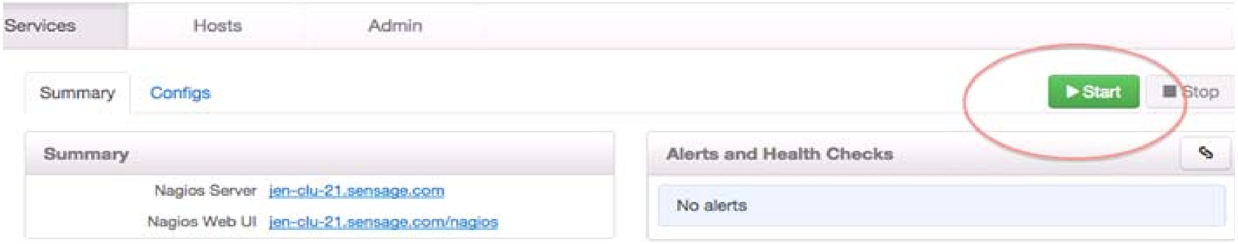
Nagios Server jen-clu-21.sensage.com
Nagios Web UI jen-clu-21.sensage.com/nagios

Alerts and Health Checks

Nagios status log staleness — OK for about 14 hours
NAGIOS OK: 2 processes, status log updated 5 seconds ago

15 Start Nagios after a successful stop.

Navigagte to services/NAGIOS/summary and click the **Start** button to start Nagios.



Summary

Nagios Server jen-clu-21.sensage.com
Nagios Web UI jen-clu-21.sensage.com/nagios

Alerts and Health Checks

No alerts

CHAPTER 5

Upgrading from HawkEye AP 5.0.1 to 6.2.0 (Needs Review)

This chapter discusses HawkEye AP product upgrade procedures and contains the following sections:

- “Considerations”, next
- “Supported Upgrades”, on page 68
- “General Upgrade Pre-checks and Restrictions”, on page 70
- “Component Upgrade Restrictions”, on page 72
- “Components Missing in the Upgrade”, on page 73
- “Backing Up and Restoring a Postgres Database”, on page 75
- “Post Upgrade Verifications”, on page 86
- “Known Upgrade and Installation Issues”, on page 87

IMPORTANT: Before you begin, please obtain the latest Release Notes for the product. This will have the most recent and up-to-date changes and bug fixes.

CONSIDERATIONS

- The "analyzer_admin" user has replaced the "hexis" user as part of the upgrade from 5.0.1 to 6.2.0.
- When upgrading, you may also need to restore any operating system or third-party configurations. For example:
    - Custom changes to `syslog-ng`
    - Nearline Storage mount points. You may need to run the `setnsi` utility. See Managing and Archiving to Nearline Storage in the *Administration Guide*.
    - SSL Certificates (Web may need to re-establish trust)
    - SSH Host Keys (ssh clients may need to re-establish trust)
    - Passwords for internal applications such as LDAP and Postgres

WARNING: You must prevent the installer (during the upgrade) from overwriting any manually-modified configuration files in the current installation.

> **NOTE:** If your files are not manually-modified, disregard instructions in this warning (as taking the following preventative measure may break the automatic configuration).

```
<5.0.1_install_prefix>/latest/jboss/server/default/deploy/postgres-ds.xml
<5.0.1 install_prefix>/latest/etc/syslog-ng/syslog-ng.conf
```

SUPPORTED UPGRADES

With HawkEye AP 6.2.0, the installer has the capability to upgrade from the following versions:

- 5.0.1 to 6.2.0

  If you are on a release prior to 5.0.1, please contact support for assistance to get you up to 5.0.1 so you can upgrade to 6.2.0.

- 6.1.0 to 6.2.0

  For details on upgrading from 6.1.0 to 6.2.0, see “Upgrading from HawkEye AP 6.1.0 to 6.2.0 (Needs Review)”, on page 89

IMPORTANT: Before upgrading any components, it is necessary to install the Deployment Manager.

If you are upgrading the OS with the product version, here is the product OS upgrade matrix:

NEED TO UPDATE DIAGRAM - PLEASE REVIEW

Figure 5-1: Certified Upgrade Paths

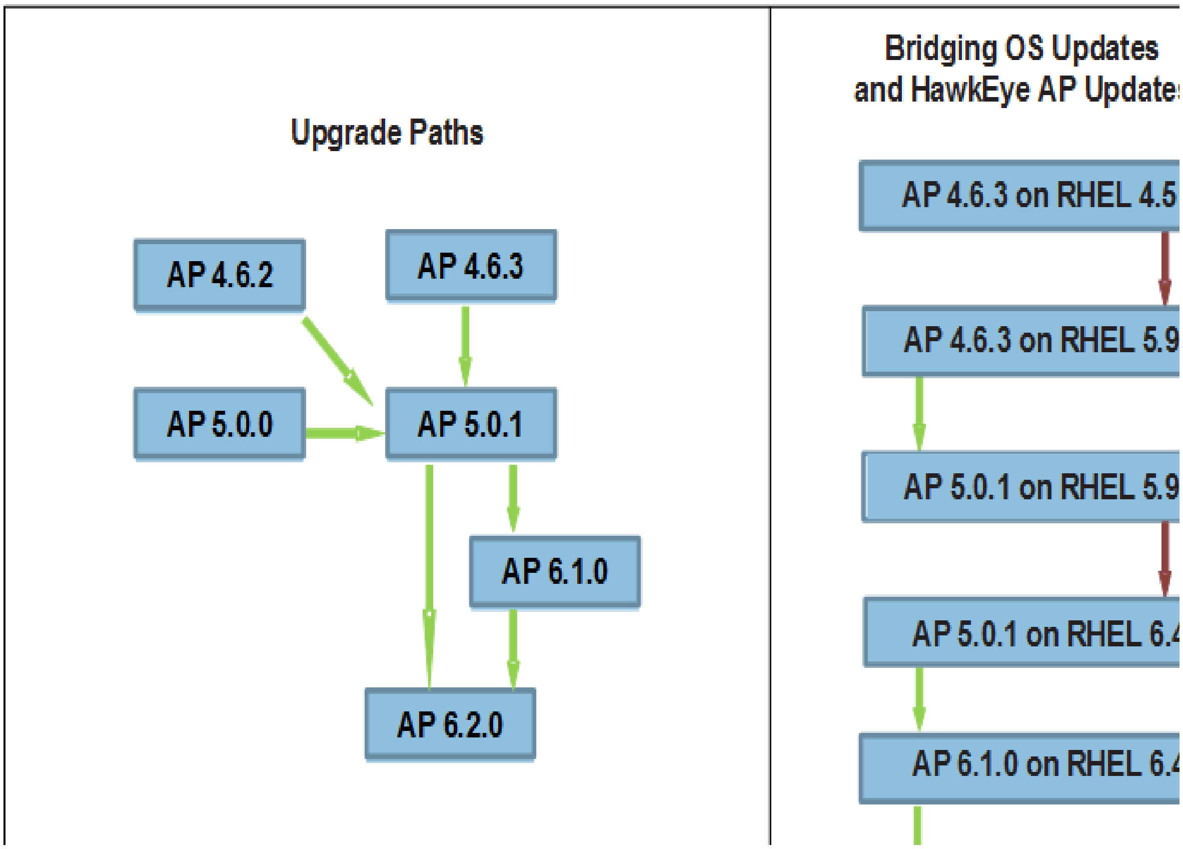
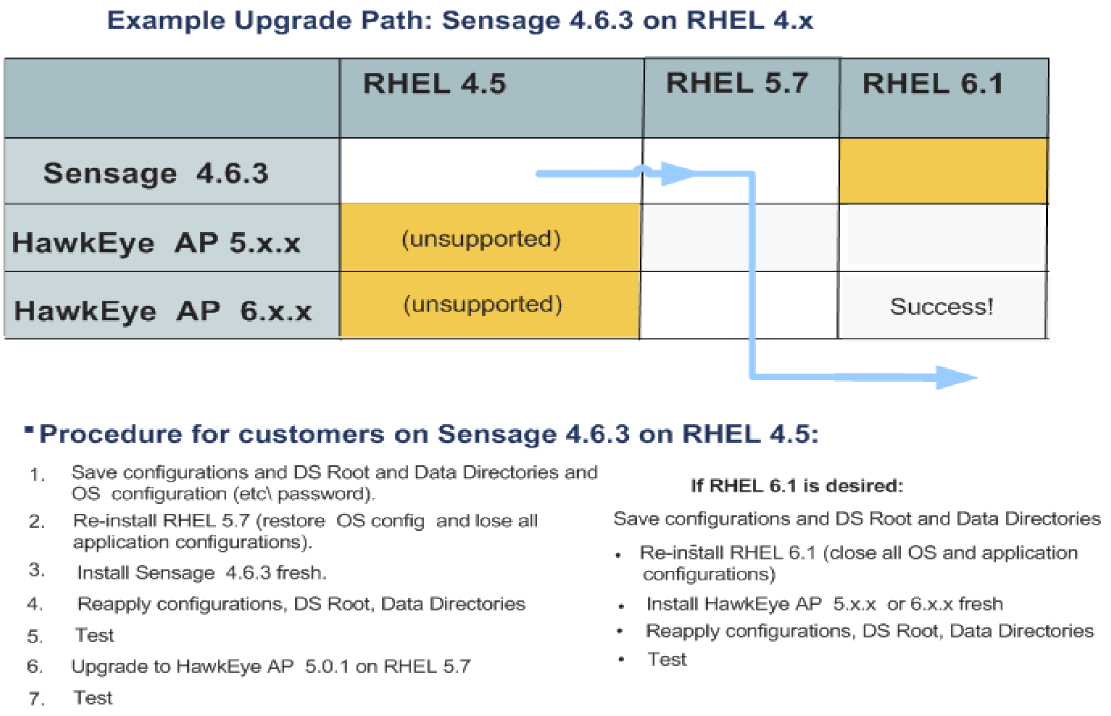


Figure 5-2 Example Upgrade Path



Example Upgrade Path: Sensage 4.6.3 on RHEL 4.x

	RHEL 4.5	RHEL 5.7	RHEL 6.1
Sensage 4.6.3			
HawkEye AP 5.x.x	(unsupported)		
HawkEye AP 6.x.x	(unsupported)		Success!

- **Procedure for customers on Sensage 4.6.3 on RHEL 4.5:**

1. Save configurations and DS Root and Data Directories and OS configuration (etc\ password).
2. Re-install RHEL 5.7 (restore OS config and lose all application configurations).
3. Install Sensage 4.6.3 fresh.
4. Reapply configurations, DS Root, Data Directories
5. Test
6. Upgrade to HawkEye AP 5.0.1 on RHEL 5.7
7. Test

If RHEL 6.1 is desired:

Save configurations and DS Root and Data Directories

- Re-inštall RHEL 6.1 (close all OS and application configurations)
- Install HawkEye AP 5.x.x or 6.x.x fresh
- Reapply configurations, DS Root, Data Directories
- Test

General Upgrade Pre-checks and Restrictions

This section contains a checklist to ensure you have met prerequisites and are aware of restrictions before beginning the upgrade.

Version Requirement

This upgrade assumes you currently have version 5.0.1 installed with the Analytics Package 1.0.7. Your 5.0.1 installation must include all hot patches up to PR-130.

Hot Patches

Prior to any 6.2.0 upgrade attempt, you must first apply all 5.0.1 hot patches. Failure to do so will have adverse consequences in HawkEye AP functionality. For example, the 5.0.1 Console will not work with Java 1.7, which is installed with the 6.1.0 upgrade.

Contact Hexis Customer Support to obtain a list of the current patches that you need to apply.

NOTE: The system is not certified or supported for patching after the 6.2.0 upgrade. Therefore do not patch up 5.0.1 after you upgrade to 6.1.0.

Upgrade Order

For upgrade from 5.0.1, components must be installed in the following order: LDAP, EDW, OAE, Collector, Analyzer (from 6.0.0 only), and Analytics (manual only). For each host, once a component has been upgraded, all other components on the same host will be broken until they are upgraded to 6.2.0 (This is because those components share RPMs and the installation location has moved.).

Login as Root

Root access is required.

AD/LDAP Integration

If you have Active Directory integration, make sure that the files that were modified are backed up. Follow the guide under "What to Backup" at the end of this section. Also be sure you have followed all preparation for setting LDAP/AD integration as noted in “Configuring Active Directory/LDAP Integration”, on page 161 of the *Administration Guide*.

Encryption

Configuration files are not encrypted.

SSL Setup

Connections to the Deployment Manager are protected by SSL, using a self-signed SSL certificate that is generated automatically during the upgrade process. The self-signed SSL certificate is set to expire in three years from the time of upgrade. You can replace the automatically generated self-signed SSL certificate with your own certificate. For details on this and managing the SSL certificate, see, “Using a Custom SSL Certificate for Deployment Manager”, on page 38 in the *Administration Guide.*

SNAPPY'PACKAGE

Before starting the upgrade, check and remove the package "snappy" if it is already installed on any of the host(s) in the cluster. Failure to do so will cause an upgrade error.

1 Run the below command to check if "snappy" is installed:

```
rpm -qa | grep snappy
```

2 Remove if "snappy" is already installed.

For example: `yum remove snappy`

LOADING DATA

Loads are not supported during an upgrade. All services except syslog-ng should be stopped before upgrading.

MOUNTED FILESYSTEMS

1 The certified filesystems are ext3 and ext4. If you are planning to use any other filesystems, please check with the Support Team.

2 If you are using a Veritas filesystem, please inform the Support Team before proceeding. You will need to download some additional scripts.

SYSLOG-NG CONFIGS

1 Please follow "What to Backup" below to ensure the syslog-ng conf files are backed up.

WHAT TO BACKUP

1 Make sure there is sufficient space to back up the Postgres, LDAP, and configuration files. For back and restore procedures, see “Backing Up and Restoring a Postgres Database”, on page 75 and “Backing Up and Restoring an LDAP Database”, on page 76.

2 Make sure that all HawkEye AP (Sensage) services are stopped.

3 Generally, it’s a good idea to create a backup folder under the installation prefix directory.

```
# <5.0.1_install_prefix>/latest/bin/clssh --hosts=<comma_delimited_hosts>
"mkdir <prefix>backup"
```

4 Back up the following folders:

```
# <5.0.1_install_prefix>/latest/bin/clssh --hosts=<comma_delimited_hosts>
"rsync -a <prefix>/etc/ <prefix>backup/etc/"
```

5 Start the HawkEye AP (Sensage) services and back up the Postgres and LDAP configuration files.

Component Upgrade Restrictions

The following are component upgrade restrictions to note when upgrading from 5.0.1 to 6.2.0.

All Components

IMPORTANT: In general, after upgrading HawkEye AP components (regardless of version), you may find some unrelated components are no longer in operation after the upgrade. Typically, you can simply restart the unrelated components.

Analytics

The Analytics upgrade is a manual procedure from 5.0.1 to 6.2.0. If you are installing Analytics, refer to "Known Upgrade and Installation Issues", on page 87. Note that AP is shipped with over 100 out-of-the-box Analytics reports that can be run and viewed in the Analyzer using the default Analyzer administrator account (admin). For a listing of available Analytics reports, see the Analytics Guide.

Collector

When adding a remote Collector host, you must add the remote Collector host to the 5.0.1 cluster before upgrading to 6.2.0; a pre-condition for upgrading remote Collectors is that the remote Collectors' configuration in the following areas are required to be the same as that of the head Collector:

- data directory
- queue directory
- state directory
- port

Before upgrading to 6.2.0 a cluster that has one or more remote Collectors, you must add the remote Collectors to the cluster if they are not already there. For details, see "Before You Begin the Upgrade", on page 77.

Event Data Warehouse (EDW)

The upgrade of the EDW is restricted in the following ways:

- Only a single instance of the EDW
- No encrypted data.
- No encrypted config file.
- No Active Directory
- **athttpd.conf** must have the following configuration settings.
  - **authenticationtype** must be set to **Default'**
  - **authenticationconf** must be set to **passphrase**
  - **authorizationtype** must be set to **Internal**
  - **fixedusersource** must be set to **slapd**
  - **CryptoMode** must be set to **none**

  - **dsroot** must be set to **`<sensage_install_prefix>/latest/data/sls/<sls_instance_name>/dsroot`**
  - **tempdir** must be set to **`<sensage_install_prefix>/latest/data/sls/<sls_instance_name>/temp`**

- **cluster.xml** must have **no inactive nodes.**
- **ldap.conf** must have the following configuration settings:
  - **dnsuffix** must be in format like:

    ```
    ou=<sensage_sls_instance>,ou=Omnisight,dc=sensage,dc=com
    ```

  - **slsdn** must be in format like:

    ```
    cn=Manager,dc=sensage,dc=com
    ```

  - **slsbindmethod** must be set to **simple**
  - **accountname** must be set to **uid'**
  - **ssl-enable** must be **yes**

Components Missing in the Upgrade

The following components are not installed or upgraded:

- Legacy Analyzer
- **clsetup** tool
- Health Check toolsr
- Real-Time System (RT)
- Single Sign-On (SSO)
- Active Directory
- Clusters with multiple EDW (SLS) instances are not supported.
- syslog-ng configuration is not upgraded.
- Collector configuration is not upgraded.

Other Notes About Upgrading Components

Review the table below for notes regarding the upgrade of specific HawkEye AP components.

Component	Note
syslog-ng	When the first HawkEye AP component is upgraded (usually LDAP), syslog-ng is also upgraded. The original <*prefix*>**/etc/syslog-ng/syslog-ng.conf** is copied to **/etc/syslog-ng/syslog-ng.conf**. The configuration is not updated. The syslog-ng install is moved from <*prefix*> to the standard location under **/**. The syslog-ng upgrade will probably result in warning messages about the configuration file being obsolete every time it is loaded. If you want to get the updated default HawkEye AP syslog-ng configuration, remove **/etc/syslog-ng/syslog-ng.conf** before upgrading a component. A new **/etc/syslog-ng/syslog-ng.conf** file will be generated from a template on each host of the upgraded component where **/etc/syslog-ng/syslog-ng.conf** is missing.
EDW	After upgrading LDAP from 5.0.1, EDW won't work until it has been upgraded.

OAE	After upgrading LDAP from 5.0.1, OAE won't work until it has been upgraded.
	The Hexis user's Postgres password is randomized during upgrade. If this affects a remote connection to the Postgres database, for example from a custom utility that connects to the controller database, it will be necessary to create a new Postgres user through which to connect. That can be done as follows on the OAE host:
	`/opt/hexis/hawkeye-ap/bin/createuser -P <new_user>`
	`su <hexis_user>`
	`/opt/hexis/hawkeye-ap/bin/psql -d <database>`
	From within PSQL, grant permissions to the new user as appropriate.

Component	Note
Collector	**After upgrading LDAP from 5.0.1, Collector won't work until it has been upgraded.** In HawkEye AP 5.0.x, there was a single Collector **config.xml** file. In HawkEye AP 6.0.x there may be any number of **config.xml** files under **/opt/hexis/hawkeye-ap/etc/collector**. Typically there will be one config.xml file directly under **/opt/hexis/hawkeye-ap/etc/collector** for global settings and another **config.xml** file for each log adapter under **/opt/hexis/hawkeye-ap/etc/collector/adapters**. **If upgrading Collector but not upgrading Analytics, note the following tasks to perform after the upgrade:** • You may need to manually update some paths at the top-level config.xml file. • Update CLIRoot to be **/opt/hexis/hawkeye-ap/bin** • You may update ConfigFile elements that point to a file under **<*old-prefix*>/etc/collector** to **/opt/hexis/hawkeye-ap/etc/collector/<*file*>** since the RPM copies these to the new location. • Update SLSSharedKey elements to **file:/opt/hexis/hawkeye-ap/etc/sls/instance/<*instance*>/shared_secret.asc**. • Update the path to atperl in any scripts referred to in config.xml. Use a command similar to: for file in **’grep -RI "\/opt\/sensage\/bin" /opt/sensage/analytics /opt/sensage/analytics’;do sed -i -e ’s/\/opt\/sensage\/bin/\/opt\/hexis\/hawkeye-ap\/bin/g’ $file;done** • Edit /opt/hexis/hawkeye-ap/bin/roll_logs.sh and set SYSLOG_DIR to the appropriate directory. **IMPORTANT: DO NOT update:** • Do not update FileRoot since the old data directory is still in use. • Do not update SourceDir *unless* the syslog-ng configuration was updated to place log files in different locations. • Do not update preprocess elements *until after* Analytics has been upgraded since the old Analytics will be left in place. • Do not update PTL location elements *until after* Analytics has been updated.
Analytics	During Analytics upgrade, a **config.xml** file is generated from a template for each log adapter. An adapters directory is created under **/opt/hexis/hawkeye-ap/etc/collector**. A link to each adapter is created under this adapters directory. The HawkEye AP 5.0.x style **config.xml** contains conflicts with many of these adapter **config.xml** files, causing Collector to fail to start. **config.xml** is renamed **config.xml.has_conflicts** and a new HawkEye AP 6.0.x style **config.xml** file is generated from template. If any of the old configuration is desired, it must be manually restored from **config.xml.has_conflicts**.

BACKING UP AND RESTORING A POSTGRES DATABASE

To back up a Postgres database:

1 Login to the Postgres host (OAE host) as the sensage user and run the following command:

```
su <sensage_user> -c '<bin_path>/pg_dump -C -f <controller_backup_file>
controller'
```

where:

<controller_backup_file> is the path where the administrator wants to store the backup

NOTE: The <*hexis_user*> for upgrades from HawkEye AP 5.0.1 is usually **lms**, or **hexis** for fresh HawkEye AP 6.x.x installs. The <*bin_path*> is <*install_prefix*>**/bin for upgrades from HawkEye AP 5.0.1** or **/opt/hexis/hawkeye-ap/bin** for fresh HawkEye AP 6.x.x installs.

2. If the new AP Analyzer is installed, additionally run:

```
su <hexis_user> -c ’<bin_path>/pg_dump -C -f <analytics_backup_file>
analytics’
```

To restore an Postgres database:

1. Login to the Postgres host and run the following command:

```
su <hexis_user> 'cat <backup_file> | <bin_path>/psql’
```

BACKING UP AND RESTORING AN LDAP DATABASE

To back up an LDAP database:

1. Login to the `atslapd` host and run the following command:

```
<prefix>/sbin/slapcat -f <prefix>/etc/atslapd/slapd.conf -l backup.ldif
```

where

<*prefix*> is <*sensage_prefix*> **on HawkEye AP 5.0.1**.

To restore an LDAP database:

1. Stop `atslapd`:

```
service sensage_atslapd stop
```

2. Remove the corrupted `atslapd` data directory.

   NOTE: You can determine what is the corrupted data directory by running the following command:

```
grep "^directory" <prefix>/etc/atslapd/slapd.conf
```

3. Create a new `atslapd` data directory:

```
mkdir <data_dir>
chown -R <hexis_user>:<hexis_user> <data_dir>
Restore:
<prefix>/latest/sbin/slapadd -f <prefix>/latest/etc/atslapd/slapd.conf -l
backup.ldif
```

4. Start atslapd:

```
service sensage_atslapd start
```

UPGRADING FROM HAWKEYE AP 5.0.1 TO 6.2.0

The following section contains the procedure to upgrade from HawkEye AP 5.0.1 to 6.2.0. While performing the upgrade, refer to relevant sections that are applicable to your upgrade, which may be a one-node or a multi-node setup.

Before You Begin the Upgrade

Before you begin the one-node or multi-node upgrade from 5.0.1 to 6.2.0, perform the following tasks:

- If you have prior versions of HawkEye AP installed on your system, be sure to bring your system environment to 5.0.1 before upgrading to 6.2.0. Contact Hexis Cyber Solutions Technical Support to obtain the correct installers.
- To meet the pre-upgrade script's dsroot and tempdir location requirements, it may be necessary to create symlinks to these directories before performing the upgrade. Check the dsroot and tempdir settings in `<prefix>/latest/etc/sls/instance/<instance_name>/athttpd.conf`. If they are set to `<prefix>/latest/data/sls/<instance_name>/dsroot` and `<prefix>/latest/data/sls/<instance_name>/temp`, this workaround can be skipped. Otherwise, follow these steps:

  a `<prefix>/latest/bin/clssh --sls-instance=<instance_name> 'ln -s <path_to_dsroot> <prefix>/latest/data/sls/<instance_name>/dsroot'`

  b `<prefix>/latest/bin/clssh --sls-instance=<instance_name> 'ln -s <path_to_tempdir> <prefix>/latest/data/sls/<instance_name>/temp'`

  c `<prefix>/latest/bin/clsetup reconfigure add sls --dsrootdir=<prefix>/latest/data/sls/<instance_name>/dsroot --sls-tempdir=<prefix>/latest/data/sls/<instance_name>/temp <instance_name>`

- Perform pre-upgrade testing:

  d Run through basic analytics "sanity" testing to ensure the majority of OOTB sources load into tables and that the data displays in reports.

  e Generate a few Real-Time alerts for OOBRules.

- If using remote Collectors, be sure to add them to the cluster if they have not already been added. To determine what Collectors have been added, execute:

  ```
  grep SENSAGE_COLLECTOR_HOST <prefix>/latest/etc/sysconfig/sensage
  ```

  All of the Collectors should be listed, including the remote ones. If not follow this procedure to add the remote Collectors to the cluster:

  f Back up **syslog-ng.conf** on all hosts:

  ```
    cp <prefix>/latest/etc/syslog-ng/syslog-ng.conf.bak <prefix>/etc/syslog-ng.conf.bak
  ```

  g Add the remote Collectors to the cluster:

  ```
    <prefix>/latest/bin/clsetup reconfigure sensage
  ```

  h Add all remote Collector hosts to the --hosts and --collector-hosts fields.

i Restore syslog-ng configuration on all hosts.

```
cp <prefix>/latest/etc/syslog-ng/syslog-ng.conf.bak <prefix>/latest/etc/
syslog-ng/syslog-ng.conf <prefix>/latest/etc/init.d/syslog-ng restart
```

Once the reconfiguration is successful, then perform the upgrade using the procedures in this chapter.

- HawkEye Retriever must be on lms-windowsretriever-5.0.1-86031.noarch.rpm. If an earlier version is installed, apply the HawkEye AP 5.0.1 patch PR-127 to upgrade it, carefully following the directions in the README.
- Obtain the **hawkeye-ap** tarball from the Hexis Cyber Solutions Support Site or your designated point of contact.

IMPORTANT NOTES about the Upgrade:

1. During upgrade from 5.0.1 components are moved from their original install prefix to `/opt/hexis/hawkeye-ap`.
2. `Syslog-ng` is moved to the normal location under **/etc/.**
3. ATSLAPD, EDW, and OAE configuration files are rewritten from templates using values read from the old configuration files.
4. The old data directories are left in their original locations.
5. When Analytics are upgraded the old config.xml is renamed as **config.xml_has_conflicts** and a new config.xml is generated.
6. Configurations from **config.xml.has_conflicts** must be manually merged into the new configuration. No scripts are provided to support this merge.
7. If your upgrade includes Analytics, make sure that you compact those tables in which you find any existence of triple buckets. To find tables with schema updates containing triple buckets, run the following command for each EDW instance:

   ```
   {code}/opt/hexis/hawkeye-ap/bin/clssh --sls-instance=<instance> find
   <data_path>/sls/<instance>/dsroot/Primary-* -name Bucket.idx{code}
   ```

8. The upgrade from 5.0.1 to 6.2.0 is performed in two states:

   1. Test the Upgrade:

   a Installs the new RPMs.

   The new RPMs are responsible for renaming any configuration files to <*file*>**.v**<*old_version*> before installing new files.

   b Configures the component per the parameter values given by Ambari which were gleaned from the old installation.

   c Depending on the component, either configures read-only mode or makes a copy of the data.

   d Starts the component.

2: Finalize the Upgrade:

a Removes all of the <*file*>**.v**<*old_version*> files.

b Depending on the component, either configures read-write mode or removes the copy of the data.

Deployment Manager

The Deployment Manager host is where the ambari-server is installed and where the HawkEye-AP repositories that are required for product upgrade are configured. You can either:

- Designate the Analyzer host of the 5.0.1 setup as the Deployment Manager host.

-OR-

- Use a separate host as the Deployment Manager.

Unpacking and Running the Upgrade Script

To unpack and run the 5.0.1 to 6.2.0 upgrade script for either the one-node or multi-node setup perform the following procedure:

1 Login to the Deployment Manager node as the root user.

2 Place the tar ball on a non-nfs mounted folder (typically under `/tmp`).

3 Be sure the root user has write permission to this directory.

4 Unpack the tarball:

```
tar -xvzf <tar_pkg>
```

5 Change the directory into the unpacked tarball folder.

```
cd hawkeye-ap
```

6 Go to Step A below for a one-node upgrade or Step B for a multi-node upgrade:

A: For a one-node upgrade:

a Install Deployment Manager and perform the upgrade with one of the following commands as follows (depending on whether you want to include Analytics in the upgrade):

Upgrade including Analytics:

```
 ./install.sh -password <Ambari password> -n <name for cluster> -e <nagios
admin_Email> (This is used by
 Nagios to send alert emails; you can change this email after upgrade if
 needed.)
```

Upgrade excluding Analytics:

```
 ./install.sh -password <Ambari password> -n <name for cluster> -e <nagios
admin_Email> (This is used by
 Nagios to send alert emails; you can change this email after upgrade if
 needed.) --dont-upgrade-analytics
```

b Follow the on screen prompts and hit the **Enter** key when prompted as noted below:

```
"Please press <enter> to continue".

This will complete the 1-node upgrade.
```

c To complete the post-upgrade steps, go to the following section: "Post-upgrade steps", on page 83.

B: For a multi-node upgrade:

a Install Deployment Manager:

```
./install.sh -password <Ambari password>
```

b Follow the on-screen prompts and hit the **Enter** key when prompted as noted below:

```
"Please press <enter> to continue".

This will complete Deployment Manager install, go to Step 7 to proceed
further with Upgrade.
```

7 Run the pre-upgrade script on the Analyzer host:

A. If the Deployment Manager is the current Analyzer host, then run the command below:

```
/tmp/hawkeye-ap/scripts/pre-upgrade.rb -o /tmp/upgrade.xml

Note: Ignore the notice displayed at the end of the pre-upgrade.rb execution.
```

B. If the Deployment Manager is on a separate host, then perform the steps below:

1. Login to the Analyzer host.

2. Copy the pre-upgrade.rb script that is available on the Deployment Manager host to the Analyzer host.

```
scp root@<deployment Manager host>:/tmp/hawkeye-ap/scripts/pre-upgrade.rb
root@<analyzer /tmp
```

4. Change the Directory to /tmp.

```
cd /tmp
```

5. Install ruby:

```
yum install ruby
```

6. Run pre-upgrade.rb script.

```
./pre-upgrade.rb -o upgrade_analyzer.xml

Note: Ignore the notice displayed at the end of the pre-upgrade.rb
execution.
```

7. Copy the `upgrade_analyzer.xml` generated in the above steps to the Deployment Manager host:

```
scp upgrade_analyzer.xml root@<deployment Manager host>:/tmp
```

8 If EDW is not hosted on the Analyzer host, perform the following tasks to additionally capture the EDW configuration:

a Login to one of the EDW hosts.

b Copy the pre-upgrade.rb script that is available on the Deployment Manager host to any one of the EDW hosts.

```
scp root@<deployment Manager host>:/tmp/hawkeye-ap/scripts/pre-upgrade.rb
/tmp
```

c Change the Directory to /tmp.

```
cd /tmp
```

d Install ruby:

```
yum install ruby
```

e Run pre-upgrade.rb script.

```
./pre-upgrade.rb -o upgrade_sls.xml
```

```
Note: Ignore the notice displayed at the end of the pre-upgrade.rb
execution.
```

f Copy the `upgrade_sls.xml` generated in the above steps to the Deployment Manager host:

```
scp upgrade_sls.xml root@<deployment Manager host>:/tmp
```

Upgrade for Multi-node Setup

To run the 5.0.1 to 6.2.0 product upgrade, perform the following procedure:

NOTE: Perform the steps below on the Deployment Manager host.

1 Install and start Ganglia Server:

a To install Ganglia Server, issue the following command:

```
hawkeye-deploy -k ~/.ssh/id_dsa --cluster=<provide cluster name> --
gangliaHost=<FQDN for Nagios Host> --targetComponent=gangliaServer --
action=install
```

NOTE:

- 1. Ganglia host can be the same as the Deployment Manager host, or one of the hosts in 5.0.1 cluster, or it can be a new host.
- 2. Cluster name should be unique, the same name should be used throughout the upgrade process.
- 3. Please see Help on hawkeye-deploy for more details about the options and its usage:

```
    hawkeye-deploy --help
```

b To start Ganglia Server, issue the following command:

```
hawkeye-deploy --targetComponent=gangliaServer --action=start
```

2 Install and start Nagios Server:

a To install Nagios Server, issue the following command:

```
hawkeye-deploy -k ~/.ssh/id_dsa --nagiosHost=<FQDN of the Nagios Host>
--targetComponent=nagiosServer --action=install --adminEmail=<nagios Admin
Email>
```

NOTE: Nagios host can be the same as the Deployment Manager host, one of the hosts in the 5.0.1 cluster, or a new host.

b To start Nagios Server, issue the following command:

```
hawkeye-deploy --targetComponent=nagiosServer --action=start
```

3 Upgrade LDAP:

a Perform the upgrade test for LDAP by issuing the following command:

```
hawkeye-deploy -k ~/.ssh/id_dsa --configFile=<provide the comma-separated
list of config file(s) generated in step 7 and/or step 8>
--targetComponent=ldap --action=upgradeTest
```

b Finalize the upgrade test for LDAP by issuing the following command:

```
hawkeye-deploy --targetComponent=ldap --action=finalizeUpgrade
```

4 Upgrade EDW:

a Perform the upgrade test for EDW by issuing the following command:

```
hawkeye-deploy -k ~/.ssh/id_dsa --configFile=<provide the comma-separated
list of config file(s) generated in step 7 and/or step 8>
--targetComponent=edw --action=upgradeTest
```

b Finalize the upgrade for EDW by issuing the following command:

```
hawkeye-deploy --targetComponent=edw --action=finalizeUpgrade
```

5 Upgrade OAE:

a Perform the upgrade test for OAE by issuing the following command:

```
hawkeye-deploy -k ~/.ssh/id_dsa --configFile=<provide the comma-separated
list of config file(s) generated in step 7 and/or step 8>
--targetComponent=oae --action=upgradeTest
```

b Finalize the upgrade for OAE by issuing the following command:

```
hawkeye-deploy --targetComponent=oae --action=finalizeUpgrade
```

6 Upgrade Collector:

a Perform the upgrade test for the Collector by issuing the following command:

```
hawkeye-deploy -k ~/.ssh/id_dsa --configFile=<provide the comma-separated
list of config file(s) generated in step 7 and/or step 8>
--targetComponent=collector --action=upgradeTest
```

b Finalize the upgrade for Collector by issuing the following command:

```
hawkeye-deploy --targetComponent=collector --action=finalizeUpgrade
```

7 Upgrade Analytics:

a Perform the upgrade test for Analytics by issuing the following command:

```
hawkeye-deploy --configFile=<provide the comma-separated
list of the config file(s)generated in step 8 and/or step 9>
--targetComponent=analytics --action=upgradeTest
```

b Perform the Post-upgrade steps in the following section, below.

Post-upgrade steps

Review the following post-upgrade steps below and follow those that are applicable to your upgrade:

1 You must perform the following post-upgrade tasks if you have upgraded Analytics:

a Gather required data for substitution as noted in the table below:

Required Data	Variable for Substitution
5.0.1 hosts {comma delimited)	{HOSTS_5.0.1}
EDW instance name	{INSTANCE_NAME}
Namespace of Analytics (usually "analytics")	{NAMESPACE}
Path to shared secret file	{SHARED_SECRET_FILE}

b Delete deprecated view:

```
/opt/hexis/hawkeye-ap/bin/atquery --verbose=1 --user=administrator
-- sharedsecret= file: {SHARED_SECRET_FILE} --namespace={NAMESPACE}
{HOSTS_5.0.1} -e ’DROP VIEW
intellischema.__connectors.webProxy__netsweeper_webFilter_sftp’
```

Example:

```
/opt/hexis/hawkeye-ap/bin/atquery --verbose=1 --user=administrator --
sharedsecret=file:/opt/hexis/hawkeye-ap/etc/sls/instance/mysls/
shared_secret.asc --namespace=analytics example.com:8072 -e 'DROP VIEW
intellischema.__connectors.webProxy__netsweeper_webFilter_sftp'
```

c Fix instance name to actual value in reports. Issue following commands on AP6_host. Please note on {INSTANCE_NAME} and {NAMESPACE} that you must replace both with appropriate values, which will depend on your 5.0.1 system. Typically, "namespace" is analytics.

```
FROM_INAME=default
FROM NS=analytics
```

```
TO_INAME={INSTANCE_NAME}
TO_NS={NAMESPACE}
PATH_TO_REPORT=/opt/hexis/hawkeye-ap/analyzer/data/reports/reports.xml

sed -i "s|\(<schemaName>\)default\(_sensage_systemanalytics</
schemaName>\)|\1${TO_INAME}\2|g" $PATH_TO_REPORT
sed -i "s|\(<schemaName>\)${FROM_INAME}_${FROM_NS}\([^<]*</
schemaName>\)|\1${TO_INAME}_${TO_NS}\2|g" $PATH_TO_REPORT
sed -i
"s|\(\"schemaName\":\"\)default_sensage_systemanalytics\([^\"]*\)|\1${TO_INAME
}_sensage_systemanalytics\2|g" $PATH_TO_REPORT
sed -i
"s|\(\"schemaName\":\"\)${FROM_INAME}_${FROM_NS}\([^\"]*\)|\1${TO_INAME}_${TO_
NS}\2|g" $PATH_TO_REPORT

unset FROM_INAME FROM_NS TO_INAME TO_NS PATH_TO_REPORT
```

d Install Analytics manually:

```
/opt/hexis/hawkeye-ap/bin/addAnalytics --sls
--src={PATH_TO_AP6_ANALYTICS} --
   namespace={NAMESPACE} --user=administrator --sls-secret=file:
   {SHARED_SECRET_FILE} --dbPassword={DB_PASSWORD}
```

Example:

```
/opt/hexis/hawkeye-ap/bin/addAnalytics --sls --src=/opt/hexis/hawkeye-ap/
analytics/ --namespace=analytics --user=administrator --sls-secret=file:/opt/
hexis/hawkeye-ap/etc/sls/instance/mysls/shared_secret.asc --
dbPassword=controller
```

2 Appserver will not start after the upgrade; apply this workaround:

a Login to the host where the old HawkEye AP Console exists.

b Run the script below:

```
/opt/hexis/hawkeye-ap/bin/update_appserver
```

c Reboot:

```
/etc/init.d/sensage_iptables start
```

3 The script **roll_logs.sh** will not work against the old location where syslog-ng’s old config file is routing data. The workaround is:

```
edit:
/opt/hexis/hawkeye-ap/bin/roll_logs.sh
replace line 16
PREFIX=$(cd$(dirname $0)/../.. && pwd)
with
PREFIX=<old Prefix>
```

4 If Ambari server does not allow a "*finalize*" after the upgrade, then the workaround is:

   a Use hawkeye-deploy to upgrade the component again.

   b Finalize before stopping the component or rebooting the host.

5 Ambari stops components that need to be running during retry, causing the retry to fail. The workaround is:

   a Use the Ambari GUI or hawkeye-deploy to start the necessary component(s) before retry.

6 Upgrade for EDW is failing on the host where only EDW is installed. The workaround is:

   a `yum --enablerepo=HAWKEYE-AP --setopt=tsflags=noscripts -y upgrade lms-atpgsql`

   b Retry.

7 If the RT parser isn't getting restarted after an upgrade from 5.0.1 nor getting started after a reboot, then the workaround is:

   a On the host containing the RT parser, issue the following command:

```
ln -s <old sensage prefix>/latest/etc/init.d/sensage_rt\
/etc/rc3.d/S85sensage_rt

/etc/rc3.d/S85sensage_rt_start
```

8 If **sensage_sls_data_dir** points to a symlink instead of the actual data directory, you may optionally reconfigure it to point to the actual data directory as follows:

   a Create a file data_dir.xml:
   `<?xml version='1.0'?><ambari><sensage_sls_data_dir>MY_DATA_PATH</sensage_sls_data_dir></ambari>`

   where you fill in **MY_DATA_PATH** with the path to your data directory. For example, if **dsroot** is at **/opt/data/sls/mysls/dsroot**, fill in /**opt/data/sls**.

   b `hawkeye-deploy --targetService=hawkeyeAP --action=reconfigure --configFile=data_dir.xml`

9 Go to the next section to install the new stack for Analyzer.

- **Install the new 6.2.0 components (Analyzer) on top of the upgraded setup.**

- **Install the new stack (Analyzer) on top of the upgraded setup.**

NOTE:

1 The following section applies to both one-node and multi-node setup.

2 Perform the steps below on the Deployment Manager host.

Installing the New Stack

To install the new stack, install and start Analyzer

1 To install Analyzer, issue the following command:

```
hawkeye-deploy --targetComponent=analyzer --action=install
-k ~/.ssh/id_dsa --configFile=/opt/hexis/hawkeye-ap/hawkeye-deploy/
sensageConfig.xml
```

NOTE: The Analyzer host should be the same as the host on which OAE is installed.

2 To start Analyzer, issue the following command:

```
hawkeye-deploy --targetComponent=analyzer --action=start
```

IMPORTANT: You must log in to the AP 6.2.0 Analyzer and create users, reports, schedules and dashboards you need. They are not automatically replicated or migrated from AP 5.0.1.

WARNING: Please be aware that scheduled reports run on AP 5.0.1 and AP 6.2.0 are independent. Running the same report on both AP 5.0.1 Console and AP 6.2.0 Analyzer causes double the load on the EDW because the same queries are sent from both AP 5.0.1 Console and AP 6.2.0 Analyzer, especially if you have a large collection of log data. You should remove the AP 5.0.1 schedules when you have verified that the equivalent schedules on AP 6.2.0 are working.

Setting up and Customizing HawkEye AP Analyzer Access

You can customize HawkEye AP Analyzer so that only users assigned to specific roles may access various Analyzer modules. For more information, see Role-Based Access to Functionality in the HawkEye AP Console in Chapter 8, “Administering Users and Authentication” in the *Administration Guide.*

If specified LDAD or AD/LDAP as your authenitication selection during the upgrade, you will also need to initially set up the Analyzer Administrator account and be sure you have used the synchronization in Analyzer to be sure Analyzer users are synched with LDAP or AD/LDAP users. For details, see

Generating Analytics Reports

The Analyzer administrator can create other user accounts in the Analyzer and grant permissions for access to these reports to selected users. By default, no users (other than the admin) have access to these reports.

Users with appropriate permissions can selectively delete reports. Note, however, that If all the reports are deleted, then all the out-of-the-box reports will be recreated the next time when the Analyzer is restarted. If you want to prevent the out-of-the-box from being recreated, you can delete the xml files in this directory: **/opt/hexis/hawkeye-ap/analyzer/data/reports/**

Alternatively, you can rename the file extension from xml to anything else. For example: **mv rc_108_reports_tags.xml rc_108_reports_tags.xml.noload**

You must do this to all the files in that directory.

Post Upgrade Verifications

Once upgrade has completed, here is a list of items to verify:

1. Make sure you have obtained a license key from support and apply it to every EDW node in your cluster.

   Once applied, you will have to restart all EDW services on all nodes.

2. Review the configs that were backed up in the section "What to Backup" in "General Upgrade Pre-checks and Restrictions", on page 70 with the current configs. If needed bring over the changes.

   a. Verify that all of the configuration files from <old_prefix>**/latest/etc/collector/** were copied to **/opt/hexis/hawkeye-ap/etc/collector/**.

3. Install or update System Analytics to ensure you can run all System Reports. Refer to *Upgrading Analytics*.

4. Verify HawkEye AP and EDW services are running all nodes.

5. Check if you can login to the HawkEye-AP 5.0.1 console via `https://<App_Server_Host>`

6. Check if you can login to the Hawkeye-AP 6.1.0 Deployment Manager via `https://<Deployment_Manager_Host>:8443`

7. Check if you can login to the Hawkeye-AP 6.1.0 Analyzer via the Analyzer web GUI link in the Deployment Manager GUI.

8. Verify Reports, Dashboards, and Libs are in working order.

9. Perform post-upgrade testing:

   a. Review reports and make sure all data that appeared in the pre-upgrade tests are still in the same reports.

   b. Run through basic analytics "sanity" testing as you did in before the upgrade; ensure all new data is loaded to the same tables and the new data shows up in reports adjacent to previous data.

   c. Run through basic 6.1.0 functionality; ensure all component status are viewable in Ambari and that all components are manageable in Ambari, and that the new Report UI works as expected.

Known Upgrade and Installation Issues

The following list shows HawkEye AP compatibility with Sun JRE 1.6 /1.7 Update versions:

HawkEye AP JRE Update Version	Compatible with corresponding Oracle JRE 1.6 or 1.7 Update
JRE 1.6_0	No
JRE 1.6 update 1	No
JRE1.6 update 2 through update 7	Yes
JRE 1.6 update 8 and update 9	No

HawkEye AP JRE Update Version	Compatible with corresponding Oracle JRE 1.6 or 1.7 Update
JRE 1.6 update 10 through 13	Yes
JRE 1.6 update 14 through 16	No
JRE 1.6 update 17 and update 18	Yes
Tested up to update 32	Yes
JRE 1.7_0	Yes

CHAPTER 6

Upgrading from HawkEye AP 6.1.0 to 6.2.0 (Needs Review)

This chapter discusses HawkEye AP product upgrade procedures and contains the following sections:

IMPORTANT: Before you begin, please obtain the latest Release Notes for the product. This will have the most recent and up-to-date changes and bug fixes.

CONSIDERATIONS

- The "analyzer_admin" user has replaced the "hexis" user as part of the upgrade from 6.1.0 to 6.2.0. DO WE NEED TO ADD MORE DETAILS TO THIS?
- When upgrading, you may also need to restore any operating system or third-party configurations. For example:
    - Nearline Storage mount points. You may need to run the `setnsi` utility. See Managing and Archiving to Nearline Storage in the *Administration Guide*.
    - SSL Certificates (Web may need to re-establish trust)
    - SSH Host Keys (ssh clients may need to re-establish trust)
    - Passwords for internal applications such as LDAP and Postgres

SUPPORTED UPGRADES

With HawkEye AP 6.2.0, the installer has the capability to upgrade from the following versions:

- 6.1.0 to 6.2.0
- 5.0.1 to 6.2.0

  If you are on a release prior to 5.0.1, please contact support for assistance to get you up to 5.0.1 so you can upgrade to 6.2.0. For details on upgrading from 5.0.1 to 6.2.0, see Chapter 5: Upgrading from HawkEye AP 5.0.1 to 6.2.0 (Needs Review)

NOTE: For upgrade from AP 6.1.0 only, individual components such as the HawkEye AP Event Data Warehouse (EDW) can be upgraded individually.

IMPORTANT: Before upgrading any components, it is necessary to install the Deployment Manager.

If you are upgrading the OS with the product version, here is the product OS upgrade matrix:

NEED TO UPDATE MATRIX - PLEASE NOTE CHANGES

Figure 6-1: Certified Upgrade Paths

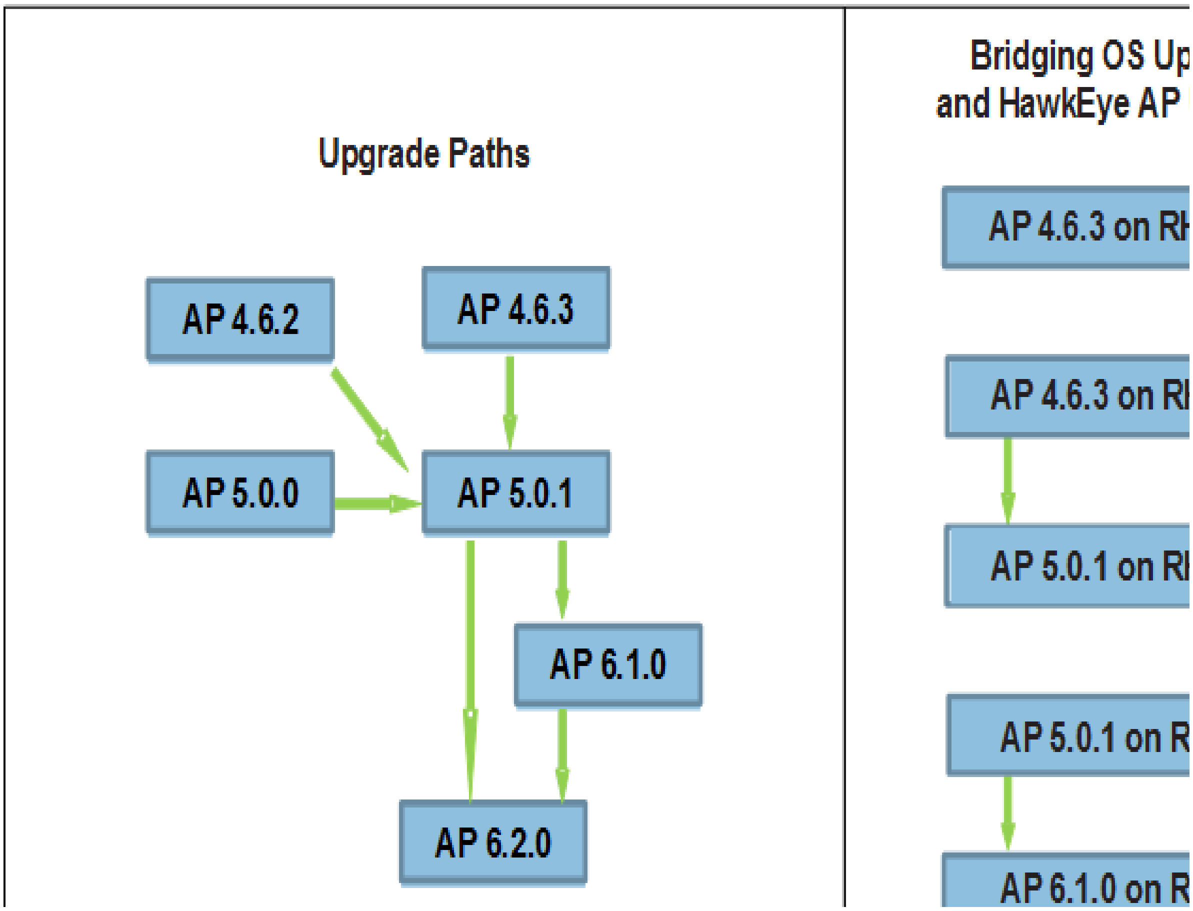
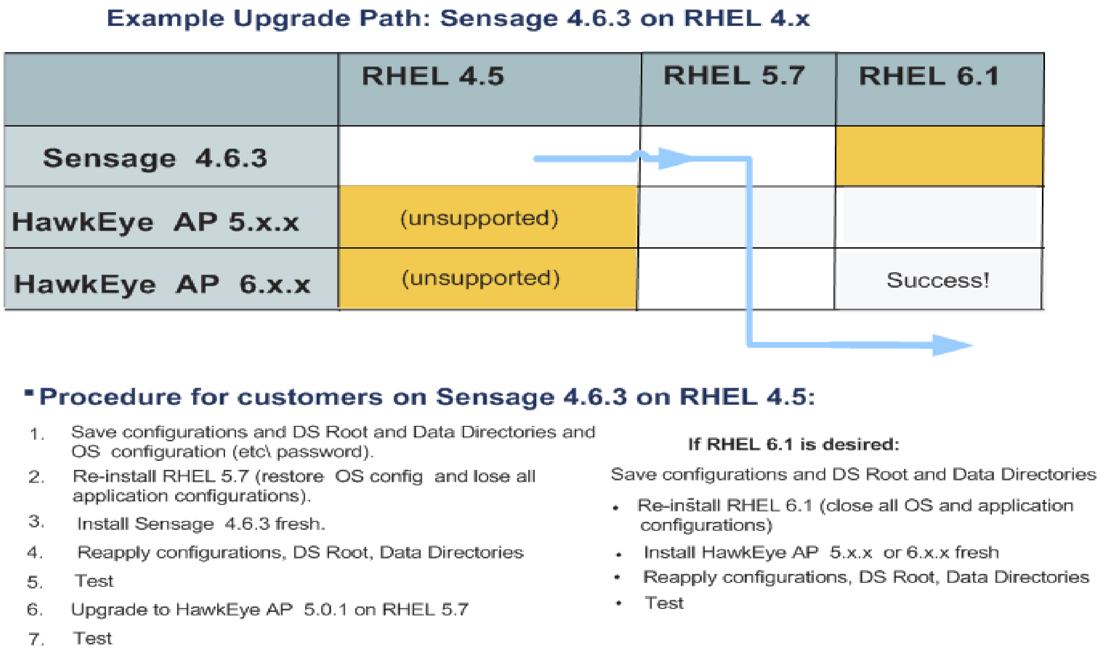


Figure 6-2 Example Upgrade Path



Example Upgrade Path: Sensage 4.6.3 on RHEL 4.x

	RHEL 4.5	RHEL 5.7	RHEL 6.1
Sensage 4.6.3			
HawkEye AP 5.x.x	(unsupported)		
HawkEye AP 6.x.x	(unsupported)		Success!

- Procedure for customers on Sensage 4.6.3 on RHEL 4.5:

1. Save configurations and DS Root and Data Directories and OS configuration (etc\ password).
2. Re-install RHEL 5.7 (restore OS config and lose all application configurations).
3. Install Sensage 4.6.3 fresh.
4. Reapply configurations, DS Root, Data Directories
5. Test
6. Upgrade to HawkEye AP 5.0.1 on RHEL 5.7
7. Test

If RHEL 6.1 is desired:

Save configurations and DS Root and Data Directories

- Re-inštall RHEL 6.1 (close all OS and application configurations)
- Install HawkEye AP 5.x.x or 6.x.x fresh
- Reapply configurations, DS Root, Data Directories
- Test

General Upgrade Pre-checks and Restrictions

This section contains a checklist to ensure you have met prerequisites and are aware of restrictions before beginning the upgrade.

Version Requirement

This upgrade assumes you currently have version 6.1.0 installed.

Upgrade Order

For upgrade from 6.1.0 to 6.2.0, components must be installed in the following order: LDAP, EDW, OAE, Collector, Analyzer, and Analytics (manual only). For each host, once a component has been upgraded, all other components on the same host will be broken until they are upgraded to 6.2.0. ((This is because we changed passwords to be more secure. Each component needs to be updated with the new passwords.)

Login as Root

Root access is required.

SSL Setup

Connections to the Deployment Manager are protected by SSL, using a self-signed SSL certificate that is generated automatically during the upgrade process. The self-signed SSL certificate is set to expire in three years from the time of upgrade. You can replace the automatically generated self-signed SSL certificate with your own certificate. For details on this and managing the SSL certificate, see, “Using a Custom SSL Certificate for Deployment Manager”, on page 38 in the *Administration Guide*.

AD/LDAP Integration

If you have Active Directory integration, make sure that the files that were modified are backed up. Follow the guide under "What to Backup" at the end of this section. Also be sure you have followed all preparation for setting LDAP/AD integration as noted in “Configuring Active Directory/LDAP Integration”, on page 161 of the *Administration Guide*.

Snappy'Package

Before starting the upgrade, check and remove the package "snappy" if it is already installed on any of the host(s) in the cluster. Failure to do so will cause an upgrade error.

1 Run the below command to check if "snappy" is installed:

```
rpm -qa | grep snappy
```

2 Remove if "snappy" is already installed.

For example: `yum remove snappy`

Loading Data

Loads are not supported during an upgrade. All services except syslog-ng should be stopped before upgrading.

MOUNTED FILESYSTEMS

1. The certified filesystems are ext3 and ext4. If you are planning to use any other filesystems, please check with the Support Team.

2. If you are using a Veritas filesystem, please inform the Support Team before proceeding. You will need to download some additional scripts.

WHAT TO BACKUP

1. Make sure there is sufficient space to back up the Postgres, LDAP, and configuration files. For back and restore procedures, see "Backing Up and Restoring a Postgres Database", on page 94 and "Backing Up and Restoring an LDAP Database", on page 95.

2. Make sure that all HawkEye AP (Sensage) services are stopped.

3. Generally, it's a good idea to create a backup folder under the installation prefix directory.

   ```
   # /opt/hexis/hawkeye-ap/bin/clssh --hosts=<comma_delimited_hosts> "mkdir /opt/hexis/hawkeye-ap/backup"
   ```

4. Back up the following folders:

   ```
   # /opt/hexis/hawkeye-ap/bin/clssh --hosts=<comma_delimited_hosts> "rsync -a /opt/hexis/hawkeye-ap/etc/ /opt/hexis/hawkeye-ap/backup/etc/"
   ```

5. Start the Sensage services and back up the Postgres and LDAP configuration files.

COMPONENT UPGRADE RESTRICTIONS

The following are component upgrade restrictions to note when upgrading from 6.1.0 to 6.2.0.

ALL COMPONENTS

IMPORTANT: In general, after upgrading HawkEye AP components (regardless of version), you may find some unrelated components are no longer in operation after the upgrade. Typically, you can simply restart the unrelated components.

ANALYTICS

If you are installing Analytics, refer to "Known Upgrade and Installation Issues", on page 106. Note that AP is shipped with over 100 out-of-the-box Analytics reports that can be run and viewed in the Analyzer using the default Analyzer administrator account (admin). For a listing of available Analytics reports, see the *Analytics Guide*.

Other Notes About Upgrading Components

Review the table below for notes regarding the upgrade of specific HawkEye AP components.

Component	Note
Analytics	During Analytics upgrade, a **config.xml** file is generated from a template for each log adapter. An adapters directory is created under **/opt/hexis/hawkeye-ap/etc/collector**. A link to each adapter is created under this adapters directory. AFTER UPGRADE FROM 6.1.0 to 6.2.0: **If you are using multiple (different) namespace**s, you must run a script to also upgrade the actual Analytics namespaces. Be sure to use the procedure noted under "Upgrading Analytics for Multiple Namespaces", on page 104.
EDW	After upgrading LDAP from 6.1.0, EDW won't work until it has been upgraded.

OAE	After upgrading LDAP from 6.1.0, OAE won't work until it has been upgraded.
	The Hexis user's Postgres password is randomized during upgrade. If this affects a remote connection to the Postgres database, for example from a custom utility that connects to the controller database, it will be necessary to create a new Postgres user through which to connect. That can be done as follows on the OAE host:
	`/opt/hexis/hawkeye-ap/bin/createuser -P <new_user>`
	`su <hexis_user>`
	`/opt/hexis/hawkeye-ap/bin/psql -d <database>`
	From within PSQL, grant permissions to the new user as appropriate.

Backing Up and Restoring a Postgres Database

To back up a Postgres database:

1 Login to the Postgres host (OAE host) as the sensage user and run the following command:

```
su <sensage_user> -c '/opt/hexis/hawkeye-ap/bin/pg_dump -C -f
<controller_backup_file> controller'
```

where: <*controller_backup_file*> is the path where the administrator wants to store the backup

NOTE: The <*hexis_user*> for upgrades from HawkEye AP 5.0.1 is usually **lms**, or **hexis** for fresh HawkEye AP 6.x.x installs.

2 If the new AP Analyzer is installed, additionally run:

```
su <hexis_user> -c '/opt/hexis/hawkeye-ap/bin/pg_dump -C -f
<analytics_backup_file> analytics'
```

To restore an Postgres database:

1 Login to the Postgres host and run the following command:

```
su <hexis_user> 'cat <backup_file> | /opt/hexis/hawkeye-ap/bin/psql'
```

Backing Up and Restoring an LDAP Database

To back up an LDAP database:

1 Login to the `atslapd` host and run the following command:

```
/opt/hexis/hawkeye-ap/sbin/slapcat -f /opt/hexis/hawkeye-ap/etc/atslapd/
slapd.conf -l backup.ldif
```

To restore an LDAP database:

1 Stop `atslapd`:

```
service sensage_atslapd stop
```

2 Remove the corrupted `atslapd` data directory.

NOTE: You can determine what is the corrupted data directory by running the following command:

```
grep "^directory" /opt/hexis/hawkeye-ap/etc/atslapd/slapd.conf
```

3 Create a new `atslapd` data directory:

```
mkdir <data_dir>
chown -R <hexis_user>:<hexis_user> <data_dir>
Restore:
/opt/hexis/hawkeye-ap/latest/sbin/slapadd -f /opt/hexis/hawkeye-ap/latest/etc/
atslapd/slapd.conf -l backup.ldif
```

4 Start atslapd:

```
service sensage_atslapd start
```

Upgrading from HawkEye AP 6.1.0 to 6.2.0

There are two different methods for upgrading to HawkEye AP 6.2.0 from HawkEye AP 6.1.0:

- If your Deployment Manager is configured to use the yum repo on **support.hexiscyber.com,** see **"Before You Begin", next**
- If your Deployment Manager is NOT configured to use the yum repo on **support.hexiscyber.com,** see **"Upgrading using a Product Tarball", on page 101**.

Before You Begin

IMPORTANT:

1 EDW service will be down after performing an Analytics upgrade. Be aware that you need to start the service manually form UI or from the command line:

a From the UI, login to the Deployment Manager and navigate to services/SENSAGE/summary tab and click the Start icon, OR

b From the command line, enter:

```
hawkeye-deploy --targetComponent=edw --action=start
```

2. If any component fails to start after an auto-upgrade, you will need to start the service manually.
3. In case the system shows that the update is available immediately after it has been applied, perform the test upgrade and apply the upgrade again.
4. Enable the adapters manually as all the adapters will be disabled after upgrade.

   Before the upgrade, make a record of the log adapters that are enabled and those you want to re-enable after the upgrade. To get the list of log adapters that are enabled, you can use the following command on the host where the Collector is installed:

   ```
   <Hawkeye AP Home>/bin/collectorAdmin enabled
   ```
5. Restart the Collector(s).

Deleting Duplicate Analytics Reports

To avoid duplication of OOTB reports you may run the following script that ***deletes*** your existing OOTB reports. After upgrading, you will receive a new set of OOTB reports. The script resides at:

```
{HawkEye_Home}/bin/report_deduplicator.rb (default path is /opt/hexis/hawkeye-
ap/bin/report_deduplicator.rb)
```

By default if the script does not accept a parameter or the parameter is missing, it will use the default value as follows:

- --hostname [HOSTNAME]
- --username [AP LOGIN USERNAME]
- --password [AP LOGIN PASSWORD]
- --path [PATH TO INSTALLED AP]
- --version [AP VERSION]

SAMPLE SCRIPT USAGE

```
./report_deduplicator.rb --hostname ap6.example.com --username
admin --password changeme --path /opt/hexis/hawkeye-ap/ --version 6.0.1
```

Upgrading using Auto-update with the support.hexiscyber.com repo

In this upgrade method, the new RPMs are located in the yum repo on support.hexiscyber.com. Perform the following steps:

IMPORTANT: Perform Steps 1-6 on the Deployment Manager host.

1. Edit /**etc/yum.repos.d/hexis.repo** and depending on the Redhat version, change the baseurl to either:

   ```
   http://support.hexiscyber.com:7748/hawkeye-ap/6.1/rhel5
   OR
   http://support.hexiscyber.com:7748/hawkeye-ap/6.1/rhel6
   ```

2 Run the following commands:

a Clear the yum cache:

```
yum clean all
```

b Stop Ambari server:

```
ambari-server stop
```

c Upgrade and install Deployment Manager RPMs:

```
yum install -y hawkeye-ap-docs-licenses mod_ssl openssl jdk1.8.0_60
yum upgrade -y lms-ambari-server lms-ambari-client hawkeye-deploy \
hawkeye-sync-rpms hawkeye-ap-docs
```

d Start Postgres

```
service postgresql start
```

e Start Ambari server:

```
ambari-server start
```

f Enable SSL on AP documentation and repository:

```
mkdir -p /etc/httpd/ssl
ln -s /var/lib/ambari-server/resources/ssl.key /etc/httpd/ssl/hawkeye-ap.key
ln -s /var/lib/ambari-server/resources/ssl.crt /etc/httpd/ssl/hawkeye-ap.crt
sed -i -e 's|http:|https:|g' -e '/sslverify=.*/d'
-e 's|\(priority.*\)|\1\nsslverify=false|g' /etc/yum.repos.d/ambari.repo
```

3 Replace **/etc/httpd/conf.d/hawkeye-ap_apache2.conf** with the following:

```
Listen 8081
MaxKeepAliveRequests 150
MaxClients 250
KeepAliveTimeout 15
MinSpareServers 10
MaxSpareServers 20
StartServers 10
MaxRequestsPerChild 500

<VirtualHost *:8081>
  DocumentRoot /var/www/html/hawkeye-ap/
  ServerName localhost
  SSLEngine On
  SSLCertificateFile /etc/httpd/ssl/hawkeye-ap.crt
  SSLCertificateKeyFile /etc/httpd/ssl/hawkeye-ap.key
</VirtualHost>
```

4 Restart httpd:

```
service httpd restart
```

5 Wait for ambari-server to finish starting up. This can be tested by trying to connect ambari-server at `https://<Deployment_Manager_host>:8443/`.

6 Synchronize the RPMs:

```
sync-rpms
```

IMPORTANT: Perform Step 7 on each Ambari agent host.

7 Execute the following commands:

a Enable SSL on the HawkEye AP repository:

```
 sed -i -e 's|http:|https:|g' -e '/sslverify=.*/d' -e
's|\(priority.*\)|\1\nsslverify=false|g' /etc/yum.repos.d/ambari.repo
```

b Clear the yum cache:

```
yum clean all
```

c Stop ambari agent:

```
ambari-agent stop
```

d Upgrade the ambari-agent

```
yum upgrade -y lms-ambari-agent
```

e Start ambari-agent

```
ambari-agent start
```

IMPORTANT: Perform Step 8-14 on the Deployment Manager.

8 Connect to the Ambari web interface and authenticate. The URL has changed to `https://<Deployment_Manager_host>:8443`.

9 In the Dashboard or Services tab expand the HawkEye AP service, which should look similar to the first screenshot below (on the left). The yellow triangles are the upgrade buttons for each component. After the upgrade has completed, a check mark icon is displayed, as shown in the second screenshot below (on the right). Click the icon to finalize the upgrade.

10 Upgrade and finalize each component in the order listed below (a-f); first click the yellow triangle for each component and then its check mark icon:

a LDAP

b EDW

c Collector

d OAE

e Analytics

f Analyzer

IMPORTANT: Failure to upgrade in this order may cause upgrade failures. In the case this has occurred, upgrade according to this listed order and then retry the failed upgrades.

11 If the system shows that the update is available immediately after applying it, perform the test upgrade and apply the upgrade again.

12 Start EDW.

13 On Analyzer host, enable the following AP system log adapters for auditing user activities on the AP system, in addition to the list of other enabled log adapters you recorded prior to the upgrade:

• hexis_hawkeye_analyzerAudit_syslogng	• sensage_sls_syslogng
• sensage_applicationManagerAudit_syslogng	• unix_ftpd_syslogng
• sensage_collectorError_syslogng	• unix_login_syslogng
• sensage_collectorTransaction_syslogng	• unix_sshd2_syslogng
• unix_su_syslogng	• unix_sudo_syslogng

For example:

```
<Hawkeye AP Home>/bin/collectorAdmin \
enable hexis_hawkeye_analyzerAudit_syslogng \
enable sensage_applicationManagerAudit_syslogng \
enable sensage_collectorError_syslogng \
enable sensage_collectorTransaction_syslogng \
enable sensage_sls_syslogng \
enable unix_ftpd_syslogng \
enable unix_login_syslogng \
enable unix_sshd2_syslogng \
enable unix_su_syslogng \
enable unix_sudo_syslogng
```

14 After you have enabled adapters, restart the Collector to pick up the changes that occurred from enabling them.

Upgrading using a Product Tarball

In this upgrade method, the new RPMs come from a product tarball and are copied to the Deployment Manager's local yum repo. Perform the following steps:

IMPORTANT: Perform Steps 1-3 on the Deployment Manager host.

1 Download the HawkEye AP 6.2.0 tarball.

2 Untar the HawkEye AP 6.2.0 tarball.

3 Execute the following commands:

a Create the directory for 6.2.0 RPMs:

```
mkdir /var/www/html/hawkeye-ap/hawkeye-ap/6.1.0
```

b Move RPMs from tarball to system directories:

```
mv -f hawkeye-ap/repo/hawkeye-ap/*.rpm /var/www/html/hawkeye-ap/hawkeye-ap/
6.1.0/
```

c Update repodata:

```
createrepo --update /var/www/html/hawkeye-ap/hawkeye-ap
```

d Clear yum cache:

```
yum clean all
```

e Stop Ambari server:

```
ambari-server stop
```

f Upgrade and install Deployment Manager RPMs:

```
yum install -y hawkeye-ap-docs-licenses mod_ssl openssl jdk1.8.0_60
yum upgrade -y lms-ambari-server lms-ambari-client hawkeye-deploy
hawkeye-sync-rpms hawkeye-ap-docs
```

g Start Postgres:

```
service postgresql start
```

h Start Ambari Server:

```
ambari-server start
```

i Enable SSL on AP documentation and repository:

```
mkdir -p /etc/httpd/ssl
ln -s /var/lib/ambari-server/resources/ssl.key /etc/httpd/ssl/hawkeye-ap.key
ln -s /var/lib/ambari-server/resources/ssl.crt /etc/httpd/ssl/hawkeye-ap.crt
mv -f <extracted_6.1.0_tarball>/hawkeye-ap/configs/hawkeye-ap_apache2.conf
/etc/httpd/conf.d/
```

```
 service httpd restart
 sed -i -e 's|http:|https:|g' -e '/sslverify=.*/d' -e
's|\(priority.*\)|\1\nsslverify=false|g' /etc/yum.repos.d/ambari.repo
```

IMPORTANT: Perform Step 4 on each Ambari agent host.

4 Execute the following commands:

a Enable SSL on the HawkEye AP repository:

```
sed -i -e 's|http:|https:|g' -e '/sslverify=.*/d' -e
's|\(priority.*\)|\1\nsslverify=false|g' /etc/yum.repos.d/ambari.repo
```

b Clear the yum cache:

```
yum clean all
```

c Stop Ambari agent:

```
ambari-agent stop
```

d Upgrade the ambari-agent:

```
yum upgrade -y lms-ambari-agent
```

e St:art Ambari agent:

```
ambari-agent start
```

IMPORTANT: Perform Steps 5-9 on the Deployment Manager host.

5 Wait for ambari-server to finish starting up. This can be tested by trying to connect to ambari-server at: `https://<host>:8443/`

6 Execute the following command:

```
for component in ldap edw collector oae analytics analyzer; do hawkeye-deploy -
-targetComponent=$component --action=upgradeTest;hawkeye-deploy --
targetComponent=$component --action=finalizeUpgrade; done
```

7 Start EDW.

8 On Analyzer host, enable the following AP system log adapters for auditing user activities on the AP system, in addition to the list of other enabled log adapters you recorded prior to the upgrade:

• hexis_hawkeye_analyzerAudit_syslogng	• sensage_sls_syslogng
• sensage_applicationManagerAudit_syslogng	• unix_ftpd_syslogng
• sensage_collectorError_syslogng	• unix_login_syslogng
• sensage_collectorTransaction_syslogng	• unix_sshd2_syslogng
• unix_su_syslogng	• unix_sudo_syslogng

For example:

```
<Hawkeye AP Home>/bin/collectorAdmin \
enable hexis_hawkeye_analyzerAudit_syslogng \
enable sensage_applicationManagerAudit_syslogng \
enable sensage_collectorError_syslogng \
enable sensage_collectorTransaction_syslogng \
enable sensage_sls_syslogng \
enable unix_ftpd_syslogng \
enable unix_login_syslogng \
enable unix_sshd2_syslogng \
enable unix_su_syslogng \
enable unix_sudo_syslogng
```

9 After you have enabled adapters, restart the Collector to pick up the changes that occurred from enabling them.

Post-upgrade steps

Review the following post-upgrade steps below and follow those that are applicable to your upgrade:

1 You must perform the following post-upgrade tasks if you have upgraded Analytics:

- **a** See "Before You Begin", on page 95 for details on **IMPORTANT** steps you must take to start up EDW service, which will be down after performing an Analytics upgrade.
- **b** See "Deleting Duplicate Analytics Reports", on page 96 for details on running a script to avoid duplication of OOTB reports.

2 If Ambari server does not allow a "*finalize*" after the upgrade, then the workaround is:

- **a** Use hawkeye-deploy to upgrade the component again.
- **b** Finalize before stopping the component or rebooting the host.

3 Ambari stops components that need to be running during retry, causing the retry to fail. The workaround is:

- **a** Use the Ambari GUI or hawkeye-deploy to start the necessary component(s) before retry.

4 Upgrade for EDW is failing on the host where only EDW is installed. The workaround is:

- **a** `yum --enablerepo=HAWKEYE-AP --setopt=tsflags=noscripts -y upgrade lms-atpgsql`
- **b** Retry.

5 If you are using multiple (different) namespaces, then you are required to perform the procedure in the following section, "Upgrading Analytics for Multiple Namespaces."

6 After you upgrade from AP 6.1.0 to AP 6.2.0, the lms-openssl package is no longer used because it has been replaced by the openssl package installed on the operating system. You should remove the lms-openssl package from AP 6.1.0 by executing the following command:

```
rpm -e lms-openssl
```

Upgrading Analytics for Multiple Namespaces

IMPORTANT: Perform the following for each additional namespace you are using for Analytics.

1 Stop Collector:

Go to Deployment Manager "Services" tab and stop Collector.

2 Run **update_tbl.pl** script.

WARNING: This script will STOP EDW.

Issue the following command on the HawkEye AP 6.2.0 host:

```
clssh --in-dir=/tmp --hosts {EDW_hosts} '{HawkEye Home}/bin/update_tbl.pl --
new-version=`rpm -q --queryformat "%{version}" lms-analytics-consumer` --
user=administrator --shared-secret=file:{shared_secret} --prefix={HawkEye
Home} --config={HawkEye Home}/etc/sls/instance/{instance_name}/athttpd.conf --
hawkeye-user={HawkEye_user} -namespace={custom_namespace}; {HawkEye Home}/etc/
init.d/sensage_edw start'
```

3 Update Connector and Master Views:

Issue the following command s on the HawkEye AP 6.2.0 host:

a

```
ATQUERY_CMD='/opt/hexis/hawkeye-ap/bin/atquery --user=administrator --
shared-secret=file:{shared_secret} --namespace={custom_namespace}
{EDW_head_host}:8072'
```

b Delete reference tables (which are empty) that contain the old schema:

```
for ref_table in \
    accountAdditionAndDeletion__windows \
    mail \
    passwordChangeAndReset__windows \
    webProxy
do

    SQLFILE=$(find /opt/hexis/hawkeye-ap/analytics/6.1.0/intellischema/ \
            -name ${ref_table}__reference.sql);
    $ATQUERY_CMD -e "DROP TABLE
    intellischema.__connectors.${ref_table}__reference";
    $ATQUERY_CMD $SQLFILE;
done
```

c Drop view for obsolete obsolete **netsweeper_webfilter_sftp** adapter:

```
$ATQUERY_CMD -e "DROP VIEW \
intellischema.__connectors.webProxy__netsweeper_webFilter_sftp"
```

d Update all connector views:

```
$ATQUERY_CMD  $(find /opt/hexis/hawkeye-ap/analytics/6.1.0/adapters/ \
-name \*__\*\.sql)
```

e Update all master view:

```
$ATQUERY_CMD  $(find /opt/hexis/hawkeye-ap/analytics/6.1.0/adapters/ \
-name \*__\*\.sql)
```

f Load report views:

```
$ATQUERY_CMD $(find \
   /opt/hexis/hawkeye-ap/analytics/6.1.0/intellischema/report_connectors/ \
   -name *\.sql \! -name \*__reference\.sql)
```

g `unset ATQUERY_CMD`

4 Start Collector:

Go to Deployment Manager "Services" tab and start Collector.

Setting up and Customizing HawkEye AP Analyzer Access

You can customize HawkEye AP Analyzer so that only users assigned to specific roles may access various Analyzer modules. For more information, see Role-Based Access to Functionality in the HawkEye AP Console in Chapter 8, “Administering Users and Authentication” in the *Administration Guide.*

If specified LDAD or AD/LDAP as your authenitication selection during the upgrade, you will also need to initially set up the Analyzer Administrator account and be sure you have used the synchronization in Analyzer to be sure Analyzer users are synched with LDAP or AD/LDAP users. For details, see

Generating Analytics Reports

The Analyzer administrator can create other user accounts in the Analyzer and grant permissions for access to these reports to selected users. By default, no users (other than the admin) have access to these reports.

Users with appropriate permissions can selectively delete reports. Note, however, that If all the reports are deleted, then all the out-of-the-box reports will be recreated the next time when the Analyzer is restarted. If you want to prevent the out-of-the-box from being recreated, you can delete the xml files in this directory: **/opt/hexis/hawkeye-ap/analyzer/data/reports/**

Alternatively, you can rename the file extension from xml to anything else. For example: **mv rc_108_reports_tags.xml rc_108_reports_tags.xml.noload**

You must do this to all the files in that directory.

Post Upgrade Verifications

Once upgrade has completed, here is a list of items to verify:

1. Install or update System Analytics to ensure you can run all System Reports. Refer to *Upgrading Analytics*.
2. Verify all HawkEye AP services are running on all the nodes as configured.
3. If the 6.1.0 system was originally upgraded from 5.0.1, then check if the 5.0.1 console is accessible via `https://<App_Server_Host>`
4. Check if you can login to the Hawkeye-AP 6.2.0 Deployment Manager via `https://<Deployment_Manager_Host>:8443`

5 Check if you can login to the Hawkeye-AP 6.2.0 Analyzer via the Analyzer web GUI link in the Deployment Manager GUI.

6 Verify Reports, Dashboards, and Libs are in working order.

7 Perform post-upgrade testing:

a Review reports and make sure all data that appeared in the pre-upgrade tests are still in the same reports.

b Run through basic analytics "sanity" testing as you did in before the upgrade; ensure all new data is loaded to the same tables and the new data shows up in reports adjacent to previous data.

c Ensure all component status are viewable in Ambari and that all components are manageable in Ambari, and that the new Report UI works as expected.

KNOWN UPGRADE AND INSTALLATION ISSUES

The following list shows HawkEye AP compatibility with Sun JRE 1.6 /1.7 Update versions:

HawkEye AP JRE Update Version	Compatible with corresponding Oracle JRE 1.6 or 1.7 Update
JRE 1.6_0	No
JRE 1.6 update 1	No
JRE1.6 update 2 through update 7	Yes
JRE 1.6 update 8 and update 9	No
JRE 1.6 update 10 through 13	Yes
JRE 1.6 update 14 through 16	No
JRE 1.6 update 17 and update 18	Yes
Tested up to update 32	Yes
JRE 1.7_0	Yes

CHAPTER 7

Removing HawkEye AP

HawkEye AP provides the uninstall.sh script to remove itself. Run the script hosts in your HawkEye AP deployment to remove your entire deployment of HawkEye AP software, including all versions that have been installed. All software, configuration, and application files are removed. Only the HawkEye AP user data directories remain after you uninstall HawkEye AP.

To completely uninstall HawkEye AP, follow these procedures:

- "Removing Your Deployment of HawkEye AP Software", next
- "Removing HawkEye AP from a Non-default Data Directory", on page 109
- "Removing HawkEye AP Windows Event Retriever", on page 109

Removing Your Deployment of HawkEye AP Software

The uninstall script must be run on each host in the HawkEye AP cluster. It removes the AP software from each host you specify, but preserves the user's data directories.

To remove all HawkEye AP user's data for each component, including EDW, Collector, LDAP, NSS, and OAE, add the `--purge` flag when running the `uninstall.sh` script.

Before you Begin

The uninstall script resides only on the Deployment Manager host. Before you begin, make a note of what hosts are in the cluster. After you run the uninstall script on the Deployment Manager host, there will be no way to know where the other hosts can be found.

- Be sure to copy `uninstall.sh` to all the other hosts in the cluster. Then run the uninstall script on each host.
- If you are uninstalling a version prior to HawkEye AP 6.0.0, be sure to generate RPMs on Deployment Manager when completing Step 3 below:

  ```
  ./uninstall.sh --generate-rpms
  ```

  IMPORTANT: If you are uninstalling a HawkEye AP 6.0.0 version you only need this step when using a 6.1.0 uninstaller to uninstall.
- If you are uninstalling from a non-default data directory, see "Removing Your Deployment of HawkEye AP Software", on page 107.

IMPORTANT: If the re-installation of AP is interrupted for any reason (power failure, user changes his/her mind on the installation, etc.), you must uninstall AP prior to any future attempts to re-install AP again.

Running the Removal Script (uninstall.sh)

To completely remove your deployment of HawkEye AP:

1 Switch to the root user:

```
su -
```

2 Change to the directory where the tarball was untarred. For example, if the tarball was untarred in **/tmp**, then:

```
cd /tmp/hawkeye-ap/
```

3 Run the following uninstall script according to your HawkEye AP deployment, specifying the parameter options below for specific directory removal. (Note that the --help option provides additional uninstall features):

```
./uninstall.sh [options]
```

a For a single-node cluster, run the uninstall script on the Deployment Manager.

b For a multi-node cluster, copy the uninstall script to each node on the cluster and run the script on each node.

NOTE: .Include the `--purge` flag to specify the deletion of user data directories. By default, the uninstall script will preserve user data in the data directories. If you want to selectively remove any of these directories, use the following parameter options in your syntax:

Parameter Options	Description
--h | --help	Prints this help menu and provides additional uninstall features; this options also lets you further customize the installation.
--purge-sls-data	Removes all EDW data.
--purge-postgres-data	Removes all Postgres data.
--purge-collector-data	Removes all Collector data.
--purge-ldap-data	Removes all EDW LDAP data.
--purge-nss-data	Removes all NSS data.
--purge	Removes all files associated with the installation. Ignore all other options.

IMPORTANT: If you plan on re-installing after the un-install, make sure that the following steps are completed before the re-install.

1 If your hosts do not have access to all dependent OS RPMs during installation, then you need to pre-install these RPMs before installation of AP starts. The dependent RPM that must be re-installed after AP is un-installed is postgressql-server RPM because it was removed when AP was un-installed.

NOTE: If your system does not have online access to RH repos, you MUST (after AP is uninstalled and prior to subsequent attempts to install AP) re-install the postgresql-server RPM before re-installing HawkEye AP.

2 Before removing the HawkEye AP installation, any existing **atslapd** data from a previous installation should be removed. If you want to preserve the data, then issue the following command:

```
mv/opt/data/atslapd /opt/data/old_atslapd
```

Then remove HawkEye AP and re-install again.

3 If you failed to remove or rename the **atslapd** data directory as mentioned in Step 2, you may experience an ldap_add_rootdc failure. The workaround to this is:

a Edit **sls.pp** and comment out the following:

```
unless=> "$sls_instance_etc_dir/ldapsearch.sh",
```

b Un-install and re-install again.

c Un-comment the line from Step 1.

d Retry the installation from the Deployment Manager GUI. If the installation does not complete successfully after you retry, you need to uninstall AP, remove/rename the **opt/data/atslapd** directory, and re-install again.

4 If Nagios cannot be started after un-installation and re-installation, issue the following command and then try to start Nagios from the Deployment Manager again.

```
rm /var/lock/subsys/nagios
```

Removing HawkEye AP from a Non-default Data Directory

If you are uninstalling from a non-default data directory such as **/opt/mydata**, the script to uninstall HawkEye AP will remove the appropriate data from the non-default data directories; note this only occurs during the first invocation of the script if you execute the script with --purge or with any of the --purge<component> data options.

After the first uninstall, should you attempt to uninstall again, the uninstall script will proceed successfully but will retain the data directories that were previously saved. (This is due to the first uninstall removing all of the necessary files the system uses to be able to detect the location of the data directories). Be sure to remove the data directories manually.

Removing HawkEye AP Windows Event Retriever

To uninstall the HawkEye AP (Sensage) Windows Event Retriever, perform the following steps:

1 Navigate to "bin" directory which is under WindowsRetriever folder:

```
cd WindowsRetriever\bin>
```

2. Run "UninstallWinRetriever.bat":

```
\\WindowsRetriever\bin>UninstallWinRetriever.bat
```

You will see the following message when execution completes:

```
wrapper | Sensage Windows Event Retriever removed.
```

```
And now this service "SenSage Windows Event Retriever" is removed from the
services.
```

APPENDIX A

INSTALLER DATA COLLECTION CHECKLIST

This appendix provides a checklist of information that you are required to provide the HawkEye AP Installer. Complete this checklist before running the installer and keep the information you've gather from this checklist on hand. This will ensure you have the information the installer needs to complete the installation.

Defining your Cluster

Check Off	Information Required	Notes
	What is the name of your cluster?	White spaces and special characters are not allowed in the name.
	What is the name of each Target Host(s) in your cluster?	
	What is the name of the file containing the SSH private key that you have set up or where is it located.	
	If you are not using the root account, provide an account that can execute sudo without entering a password.	
	All the services listed must be installed.	These services are required to run HawkEye AP:
	Choose the components that your want to install on each host of your HawkEye AP cluster	Refer to your HawkEye Deployment Type
	What master components will run on each host? The master components are Ganglia, Nagios, LDAP, and OAE.	
	What slave components will run on each host? The slave components are EDW and Collector.	

Check Off	Information Required	Notes

Installation, Configuration, and Upgrade Guide

INDEX