ExtremeManagement™

Deploying Extreme Fabric Orchestrator

Release 1.2
NN48100-101
Issue 03.01
December 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: http://www.extremenetworks.com/support under the link ""Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Extreme Networks, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Extreme Networks' prior consent and payment of an upgrade fee.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks' website at:http://www.extremenetworks.com/support/policies/software-licensing or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at https://gtacknowledge.extremenetworks.com/.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: http://documentation.extremenetworks.com, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website:http://www.extremenetworks.com/support for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website:http://www.extremenetworks.com/support/contact/ (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: http://www.extremenetworks.com/company/legal/

Contents

Chapter 1: Preface

Purpose

This document contains concepts, operations, and tasks related to the deployment and configuration of the appliance.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to http://www.extremenetworks.com/support/service-notification-form/ .
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: New in this document

The following sections detail what is new in *Deploying Extreme Fabric Orchestrator*, NN48100–101. See *Extreme Fabric Orchestrator Release Notes* for a list of supported features.

Upgrade process

The process to upgrade EFO infrastructure is updated to support upgrades from Release 1.0 or 1.1 to Release 1.2. Once upgrade bundles are downloaded and transferred to the Server, you can initiate a system upgrade from the KVM hypervisor CLI using an iLO console connection or local connection to the Server. The upgrade process supports Standalone and High Availability system configurations.

Note:

A new EFO appliance ships with a prior release. You must deploy and configure the EFO appliance before upgrading to Release 1.2.

Data migration changes

Data migration from legacy applications is not supported in EFO Release 1.2. EFO Release 1.1 and 1.0 supports legacy application data migration. You must migrate legacy application data before upgrading to EFO Release 1.2.

Chapter 3: End-to-end process overview

EFO end-to-end process workflow

The following section depicts end-to-end pre and post deployment high-level process workflow of Extreme Fabric Orchestrator (EFO) at a customer location.

Note:

The EFO appliance ships with Release 1.1 software. You must deploy and configure Release 1.1 before upgrading to Release 1.2.

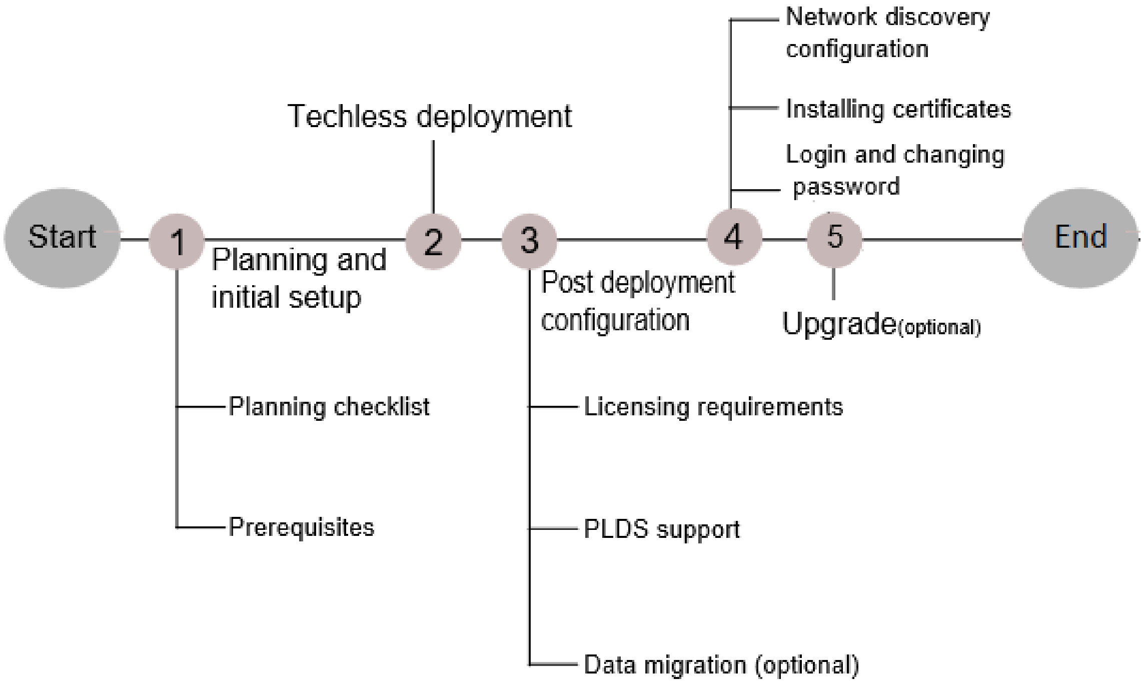

Network discovery configuration
Installing certificates
Login and changing password
Techless deployment
Start
1
Planning and initial setup
2
3
Post deployment configuration
4
5
Upgrade(optional)
End
Planning checklist
Prerequisites
Licensing requirements
PLDS support
Data migration (optional)

Figure 1: EFO process workflow diagram

Chapter 4: Planning and initial setup

Planning checklist

Use this checklist to track each step required to deploy an Extreme Fabric Orchestrator (EFO). See *Extreme Fabric Orchestrator Release Notes* for feature support.

Before you start a new Extreme Fabric Orchestrator (EFO) configuration, print the checklist. Check the steps as you complete them to make sure that you do not overlook any important task.

Table 1: Planning checklist

No.	Task	Comments	✔
1	Assemble the appliance and read the enclosed *HP ProLiant DL360 Gen9 Server* setup overview information.	EFO is a hardware appliance that operates virtualized management modules on a RHEL KVM Hypervisor. For more information and instructions on installing and commissioning a factory-supplied Extreme Fabric Orchestrator (EFO) appliance, see *Getting Started and Locating the latest software and Release Notes for Extreme Fabric Orchestrator*, NN48100–102.	
2	Gather the necessary cables and equipment.	• Minimum of two Ethernet cables (minimum of three for High Availability) for each appliance • Monitor • Keyboard	
3	When installing the appliance in a rack, select a location that meets the environment standards described in *HP ProLiant DL360 Gen9 Server User Guide*.	To ensure continued safe and reliable equipment operation, install or position the system in a well ventilated, climate-controlled environment.	

Chapter 5: Techless deployment

Deploying EFO Standalone

About this task

Perform the following procedure to deploy an EFO appliance as a Standalone Leader node. You can configure the appliance with a keyboard, video, and mouse locally.

Procedure

1. Ensure the EFO appliance NIC1 is connected to the management network, and power on.

   ✱ **Note:**

   The appliance is configured to boot into the installer. Do not press any keys until the Extreme Networks software license terms display.

2. Click `Enter` to read the Extreme Networks software license terms.

3. On the **End User License Agreement (EULA)** screen, review the EULA and press `space` to continue until prompted to accept the Extreme Networks Software License Terms. Enter `Y` to accept the license agreement and proceed with the installation.

   ✱ **Note:**

   If you enter `N`, the installation aborts and the EFO appliance cannot be deployed.

4. On the **Appliance Network configuration** section, Enter `1` to select a New/Standalone Node.

   ✱ **Note:**

   If you want to enable High Availability (HA), you must complete a Standalone configuration first. Then you can install a HA license and proceed to deploy the second appliance to join HA cluster as standby node, see Deploying EFO High Availability on page 16.

5. Choose and enter a **Networking Configuration type**:

Choice Option	Choice Description
1	Same Network for EFO Services and HP Integrated Lights-Out (iLO)
2	Different Network for EFO Services and HP Integrated Lights-Out (iLO)

Note:

If you select Option 2, you must provide an IP address range, then enter the iLO IP address, iLO netmask, and iLO gateway addresses as prompted.

6. In the **KVM Configuration Parameter** section, do the following:
   a. Enter the prefix name for the appliance for auto generating the FQDN.
   b. Enter the domain name for the appliance for auto generating the FQDN.

      Note:

      The FQDN length must not exceed 40 characters.
   c. Enter the IP address of your DNS server (Optional).
   d. Enter the IP address of your NTP server (Optional).
   e. Select a continent or ocean to configure the time zone.
   f. Select a country.
7. In the **Application Network Configuration Details** section, do the following:
   a. Enter an IP address range of at least ten unused IP addresses for configuring the list of applications displayed. You can enter multiple IP addresses separated by a comma, or an IP range separated with a dash. See the example provided on screen.

      Note:

      If you chose option 2 in step 5, enter an IP address range of at least nine unused IP addresses.

      The system automatically assigns the IP addresses in sequence and appends the domain name to the auto-generated short hostname.
   b. Enter the Netmask, typically `255.255.255.0`.
   c. Enter the IP address for the default gateway.

      Note:

      If you chose option 2 in step 5, you are prompted to enter a separate iLO IP address, netmask, and default gateway.
8. A choice to configure a second network displays. `Do you want to configure separate network than the appliance management network for managing devices? [y/n]:`

Choice Option	Choice Description
N	One applications and devices network (Proceed to Step 9)
Y	Creates two applications and devices networks (Perform Step 8 substeps to configure the second network)

   a. In the **Application Second Network Configuration Details** section, enter an IP range of at least six unused IP addresses for configuring the list of applications displayed. You can enter multiple IP addresses separated by a comma, or an IP range separated with a dash. See the example provided on screen.

b. Enter the Netmask, typically `255.255.255.0`

c. Enter the IP address for a second gateway (Optional)

9. The **Appliance Network Configuration** summary screen displays the IP addresses, FQDNs for the applications, and (if a second network was selected) the managed device network.

   Important:

   After completing the configuration, add the listed **IP Addresses** and **FQDNs** on your DNS server.

10. On the **Appliance Network Configuration** summary screen review the network configuration summary and choose the appropriate option:

Choice Option	Choice Description
y	Enter `y` to proceed with the configuration.
e	Enter `e` to edit configuration parameters.
x	Enter `x` to exit configuration and shutdown the server.

11. If you choose `y` to start the configuration, the system starts the reboot. It takes approximately 45 minutes to complete the configuration.

    The system displays the configuration status as `Deployment Successful` or `Deployment Failure`.

    - If the configuration status is `Deployment Successful`, the system displays the service FQDN details to launch the EFO application in the web browser.

Next steps

Perform a health check to ensure all the applications are configured successfully and everything is functional. For more information, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

Configuration flowchart

The following flowchart depicts the initial steps for configuring Extreme Fabric Orchestrator (EFO).

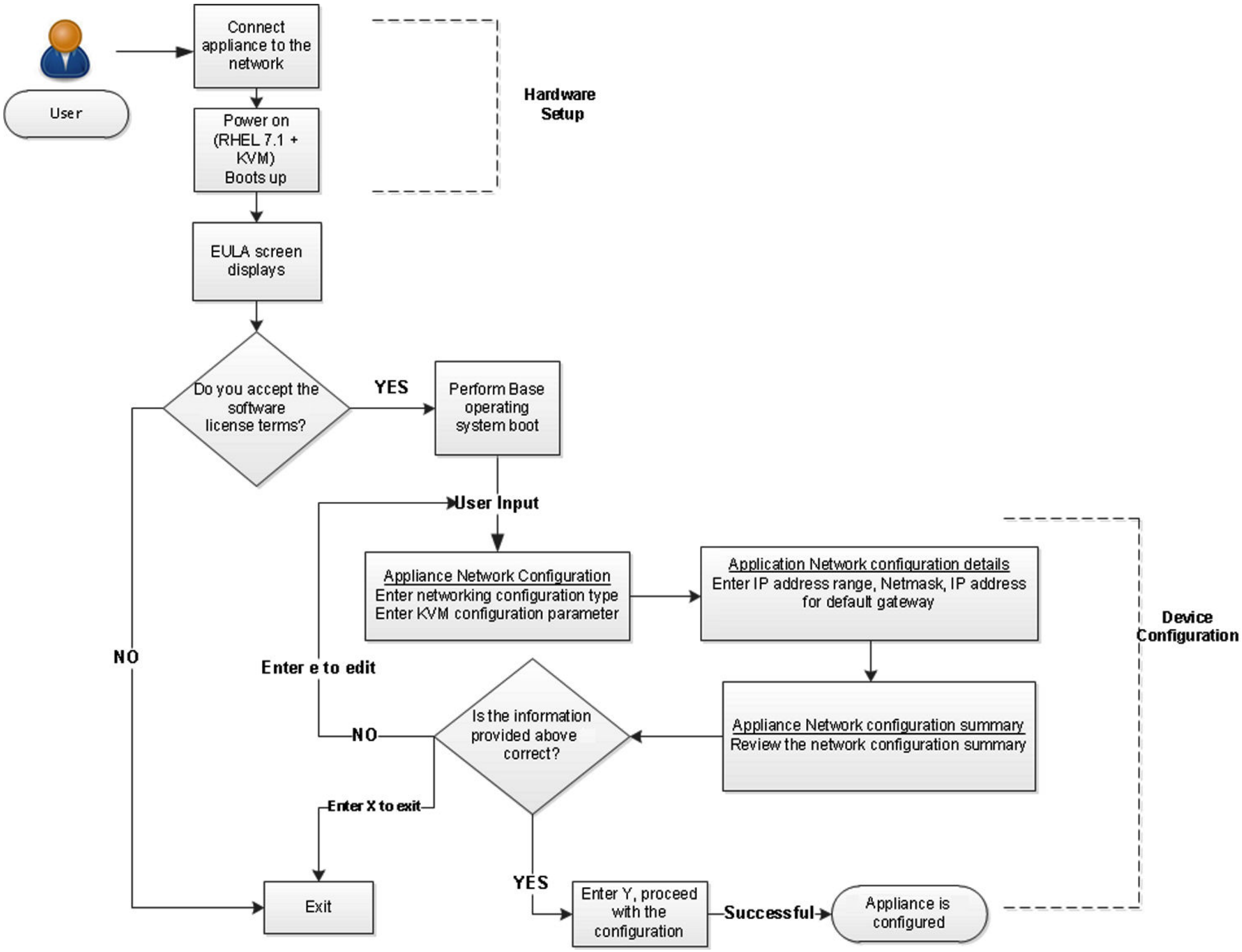

User
Connect appliance to the network
Power on (RHEL 7.1 + KVM) Boots up
Hardware Setup
EULA screen displays
Do you accept the software license terms?
YES
NO
Perform Base operating system boot
User Input
Appliance Network Configuration
Enter networking configuration type
Enter KVM configuration parameter
Application Network configuration details
Enter IP address range, Netmask, IP address for default gateway
Device Configuration
Enter e to edit
Appliance Network configuration summary
Review the network configuration summary
Is the information provided above correct?
NO
Enter X to exit
YES
Exit
Enter Y, proceed with the configuration
Successful
Appliance is configured

Figure 2: EFO Configuration flowchart

Deploying EFO High Availability

About this task

Perform the following procedure to deploy an EFO appliance as a Standby Master node for an EFO High Availability (HA) configuration. You can configure the appliance with a keyboard, video, and mouse locally, or with an iLO connection configured for remote console access.

Before you begin

- You must deploy and configure the EFO Standalone Leader node before you can deploy HA. See Deploying EFO Standalone on page 13.
- You must purchase and install an EFO High Availability license on the Standalone Leader node before you can deploy the Standby Master node.
- Ensure the EFO Standalone Leader node is powered on and EFO is operating.

- Ensure the EFO dashboard password is reset from default.
- Ensure both EFO appliances have NIC1 connected to the same management network.
- Ensure both EFO appliances have NIC3 connected to each other, either directly with a crossover Ethernet cable, or through a private network.
- (Optional) Ensure both EFO appliances have NIC2 connected to the device network.

Procedure

1. Power on the EFO Standby Master appliance and wait for boot sequence to complete.

   Note:

   The appliance is configured to boot into the installer. Do not press any keys until the Extreme Networks software license terms display.

2. Click `Enter` to read the Extreme Networks software license terms.
3. On the **End User License Agreement (EULA)** screen, review the EULA and press `space` to continue until prompted to accept the Extreme Networks Software License Terms. Enter `Y` to accept the license agreement and proceed with the installation.

   Note:

   If you enter `N`, the installation aborts and the EFO appliance cannot be deployed.

4. On the **Appliance Network configuration** section, Enter `2` to choose to join HA cluster as standby.
5. Enter the **Integration IP** of the Leader KVM Server. Default is `10.10.10.1`. Press `Enter`.

   Communication with the EFO Leader node is established and the EFO HA license is validated. If no HA license is detected you are prompted to install the license before you can continue the configuration. If the HA license is detected, the configuration continues.

   Note:

   A Standalone Leader node with an EFO HA license installed is required to deploy the Standby node for a HA configuration.

6. Enter a **Management Network** IP address for the Standby node. A subnet is shown based on the Leader node configuration. Enter an `<A.B.C.D>` IP address valid for the subnet range shown.
7. Enter a **HP Integrated Lights Out (iLO) Network** IP address for the Standby node. Enter an `<A.B.C.D>` IP address valid for the subnet range of the Management Network.
8. Enter a **Netmask** IP address. Default is `255.255.255.0`. Press `Enter`.
9. Enter a **Default Gateway** IP address. A default is shown based on the Leader node configuration. Press `Enter`.
10. Enter the **EFO Dashboard Administrator Password**. Enter the Leader node `<password>` for the administrator account of EFO.

11. The **Appliance Network Configuration** summary screen displays the IP addresses and FQDNs for the applications.

    Important:

    After completing the configuration, add the listed **IP Addresses** and **FQDNs** on your DNS server.

12. On the **Appliance Network Configuration** summary screen review the network configuration summary and choose the appropriate option:

Choice Option	Choice Description
y	Enter `y` to proceed with the configuration.
e	Enter `e` to edit configuration parameters.
x	Enter `x` to exit configuration and shutdown the server.

13. If you choose `y` the system starts the Standby node configuration. It takes approximately 20 minutes to complete the initial configuration.

    Important:

    Once the Standby node configuration is complete, the data replication process begins. Data replication takes approximately 20 minutes to complete. HA failover is not available until the data replication is completed.

14. Check the High Availability status. Establish an SSH or console connection to the KVM hypervisor and login as root. Execute the following command `bash /usr/local/infra/bin/ha_status.sh` and view the replication status.

Next steps

Perform a health check to ensure all the applications are configured successfully and everything is functional. For more information, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

Chapter 6: Post-deployment configuration

EFO licensing

Licensing in EFO uses the System Manager WebLM as the license server to add or remove licenses.

Each EFO appliance requires a license. The licenses are node locked to the appliance and the WebLM server, hence they cannot be transferred from one appliance to the other. The type of license you purchase determines the device count and features available for each application. The Advanced Monitoring license includes all of the applications and features.

Important:

High Availability (HA) requires a HA license installed on the leader EFO appliance. For HA the standby EFO appliance does not require additional stand-alone node licenses.

License activations in PLDS require the HostID of the WebLM server and Monitoring VM HostID for inclusion in the license file. The HostID of the WebLM server is displayed on the Server Properties page of the WebLM.

License type

The following list outlines the types of EFO licenses:

- 250-Node

  Important:

  - Carefully consider your starting license. You cannot go from the 250–Node license to the 1500–Node license by way of an EFO upgrade. If you know that you will need more than 250 nodes, start with the 1500–Node license.
  - EFO supports upgrade from 1500–Node license to 5000–Node license.
- 1500-Node
- 5000-Node
- Additional 10000–Node for Monitoring
- High Availability

The following table outlines the device count for each module.

Table 2: Device count for modules

Application	250-Node	1500-Node	5000-Node
Configuration	250	1,500	5,000
Monitoring	1,000	6,000	• The device count is 20,000 (without +10000 Monitoring add-on license) • The device count is 30,000 (with +10000 Monitoring add-on license)
IP Flow	10	10	10
Virtualization	220	220	220

The following table outlines the device count for the EFO Monitoring module.

Table 3: Device counts for Monitoring

Managed Devices	250-Node	1500-Node	5000-Node
Extreme Networks Switches	250	1,500	5,000
UC, CC, phones, Extreme Networks solution (EMC, HP), Servers, VMs, 3rd party Switches, other managed objects	750	4,500	• The device count is 15,000 (without +10000 Monitoring add-on license) • The device count is 25,000 (with +10000 Monitoring add-on license)
Total	1,000	6,000	• 20,000 (5,000+15,000) • 30,000 (25,000+5,000)

Additional features

At the time of acquiring a license, you must select any additional features you wish to access along with the license type. This include the Advanced Monitoring features.

The Advanced Monitoring feature is available for all license types and can be enabled or disabled based on your requirement.

If you wish to purchase any additional features after you acquire a license, you can contact Avaya support to receive a new license for EFO from PLDS. You must replace the existing license with the new license on the WebLM server.

Trial version

EFO provides a trial version of 15 days which will be available soon after the configuration of EFO on the hardware appliance for the first time. You do not require any trial license file to run the trial version. The standard license will be active during the trial period.

Grace Period

A grace period of 30 days is available in case of any of the following scenarios :

- The absence of a valid license after the trial period expires or at any given time.
- If after installing license there is any loss of connectivity to the license (WebLM) server.

For more information about licenses, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

PLDS support

Avaya Product Licensing and Distribution System (PLDS) enables you to perform licensing and entitlement management.

All licensing activities are performed through the Avaya PLDS Portal at http://plds.avaya.com.

License procurement workflow

About this task

This work flow shows you the sequence of tasks you perform to generate a new license for Extreme Fabric Orchestrator (EFO).

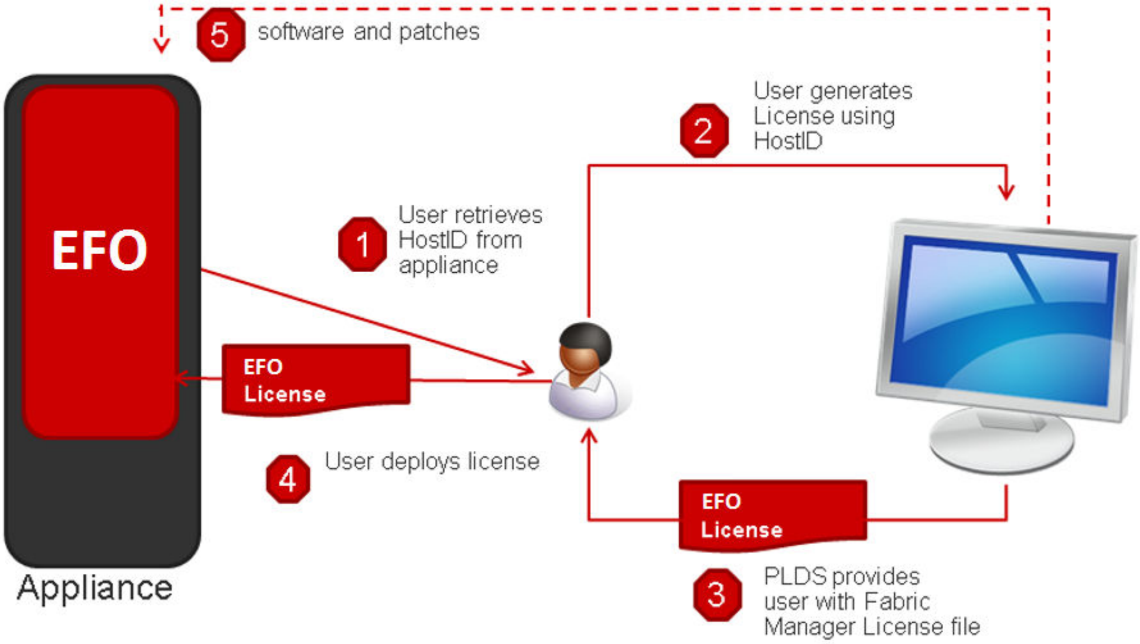

5 software and patches
EFO
Appliance
2 User generates License using HostID
1 User retrieves HostID from appliance
EFO License
4 User deploys license
EFO License
3 PLDS provides user with Fabric Manager License file

Figure 3: License Procurement workflow

Before you begin

- Login to KVM as a root user using the Command Line Interface (CLI).

Procedure

1. Run the **`afo-hostid`** command to generate the HostID for the WebLM server.

   You can obtain the HostID from MSC CLI as well as from EFO's About dialog.

2. Using this HostID, generate a license in Avaya Product Licensing and Distribution System (PLDS).

   All licensing activities are performed through the Avaya PLDS Portal at http://plds.avaya.com.

3. PLDS provides a Fabric Manager License file.

4. Use this license file to install the licenses in EFO.

5. **(Optional)** You can auto-download entitlements from PLDS. You can also auto-download patches and new software from PLDS using Management Server Console (MSC).

Next steps

For more information about obtaining and installing a web-based license manager (WebLM) from Extreme Fabric Orchestrator (EFO), see *Administration using Extreme Fabric Orchestrator*, NN48100–600.

Chapter 7: Data migration

Overview of migration to EFO

Migration is the process of carrying over data from an older application to a newer version of Extreme Fabric Orchestrator (EFO). You can choose to migrate to EFO if you are currently using any legacy application as mentioned in the table below.

EFO enables you to migrate device credentials and other platform data such as users from legacy applications.

Important:

Legacy application data migration is not supported in EFO Release 1.2. EFO Release 1.1 and 1.0 supports legacy application data migration from the following versions. You must migrate legacy application data before upgrading to EFO Release 1.2.

Supported migration versions

EFO supports migration from the following legacy application versions.

Table 4: Supported migration

Applications	Version number
Configuration & Orchestration Manager (COM)	3.0.2, 3.1, 3.1.1, 3.1.2, and 3.1.3
Virtualization Provisioning Service (VPS)	1.0.2, 1.0.3, and 1.1
IP Flow Manager (IPFM)	2.0.2 and 2.1
Visualization, Fault & Performance Manager (VPFM)	3.0.3.1, 3.0.3.2, 3.0.3.3, and 3.0.4

Migration process

1. Back up the older applications (legacy cluster) data.
2. Migrate data from the older applications (legacy cluster) to EFO.

Backup methods

Backup of legacy cluster to EFO is performed using the manual backup. For more information on manual backup, see Performing manual backup on page 24.

Performing manual backup

About this task

You can perform this task manually on the following Windows or Linux based legacy clusters:

- Unified Communications Manager (UCM)
- System Manager (SMGR)

Before you begin

- Ensure that you have the `Migration_From_Legacy_To_AFO_PLUS.zip` file.

  ⊕ **Tip:**

  Download the latest file from the support site.

- Extract and check for the following list of files in the `Migration_From_Legacy_To_AFO_PLUS.zip` file:
  - `LegacyDataCollector.pl`
  - `Migration_From_32Bit_UCM_To_SMGR-CS.zip`
    - `ucm-to-smgr-migration-linux.zip`
      - `bin - > backupDataMigration.sh, ucmcsexport.sh`
      - `lib -> ecc-module-backup.jar`
    - `ucm-to-smgr-migration-windows.zip`
      - `bin -> backupDataMigration.bat, ucmcsexport.bat`
      - lib -> ecc-module-backup.jar
    - `README.txt`

Procedure

1. Login to the legacy cluster (UCM or SMGR) using the Command Line Interface (CLI).

   ✱ **Note:**

   For more information on how to perform legacy applications backup, see Performing Backup for Legacy applications on page 25.

2. Run **`LegacyDataCollector.pl`** on your legacy cluster, to generate an archive of the legacy data.

   The following table lists the files that are generated on the legacy cluster:

Legacy Cluster	Files
On UCM based system	The archive of legacy cluster is available on `/opt/avaya/UCM/backups` and include the following list of files: • `JbossQuantumMigration.zip` • `a` *`<date>`*`_`*`<time>`*`.jar file`

Legacy Cluster	Files
	• `MetaData.properties file`
On SMGR based system	The archive of legacy cluster is available on `/opt/avaya/smgr/backups` and include the following list of files: • `MgmtBackup_6.3.8.tar.gz` • `a <date>_<time>.jar file` • `MetaData.properties file`

Note:

The properties file generated by the legacy cluster includes the legacy application details.

3. Copy the backup archives on the EFO MSC server to restore the data. For more information, see Migrating and restoring data on page 27.

Related links

Performing backup of legacy applications on page 25

Performing backup of legacy applications

About this task

Use this procedure to perform backup of the legacy applications for UCM and SMGR based legacy system.

Note:

- If the legacy application is a Windows machine, extract `ucm-to-smgr-migration-windows.zip`
- If the legacy application is a Linux machine, extract `ucm-to-smgr-migration-linux.zip`

Procedure

1. For UCM based legacy system,

   If the legacy application machine is Windows based :

   a. Login to Windows based machine.

   b. Unzip the zip files in the UCM home directory.

   c. Copy the script files in the `bin directory`.

   d. Copy the jar files in the `lib directory`.

   e. On the UCM home directory, execute the command :**`LegacyDataCollector.pl`** and enter the `admin` password.

If the legacy application machine is Linux based :

a. Login to Linux based machine.

b. Unzip the zip files in the UCM home directory.

c. Copy the script files in the `bin directory`.

d. Copy the jar files in the `lib directory`.

e. Grant permissions to execute the following commands:

- `chmod +x ucmcsexport.sh`
- `chmod +x backupDataMigration.sh`

f. On the UCM home directory, execute the command :**`LegacyDataCollector.pl`** and enter the `admin` password.

2. After successful completion of the command, following files are generated in the `UCM_HOME/backups` for the Windows based machine and `/opt/avaya/ucm/backups` for the Linux based machine:

   - `<date>_<time>.jar`
   - `JbossQuantumMigration.zip`
   - `MetaData.properties file`

3. For SMGR based legacy system,

   If the legacy application machine is Windows based :

   a. Login to Windows based machine.

   b. Copy **`LegacyDataCollector.pl`** to the `SMGR_HOME/bin folder`, here SMGR_Home is Product installation directory.

   c. Execute the **`LegacyDataCollector.pl`** command.

   If the legacy application machine is Linux based :

   a. Login to Linux based machine.

   b. Copy **`LegacyDataCollector.pl`** to the `/opt/avaya/smgr/bin` directory.

4. After successful completion of the command, following files are generated in the `/opt/avaya/smgr/backups` folder:

   - MgmtBackup_6.3.8.tar.gz
   - `<date>_<time>.jar`
   - `MetaData.properties`

Next steps

Perform migration of the legacy data into EFO.

Related links

Performing manual backup on page 24

Migrating and restoring data

About this task

After you back up the legacy cluster, perform this task to migrate and restore data. You can migrate the following data on the EFO cluster:

- Users

  Note:

  The system migrates users associated with the system administrator, UCM system administrator, UCM operator, and Network administrator.

- Device credentials

  Note:

  The system automatically does not restore the device credentials file from the backed up file. You need to perform a manual restore.

- Application data

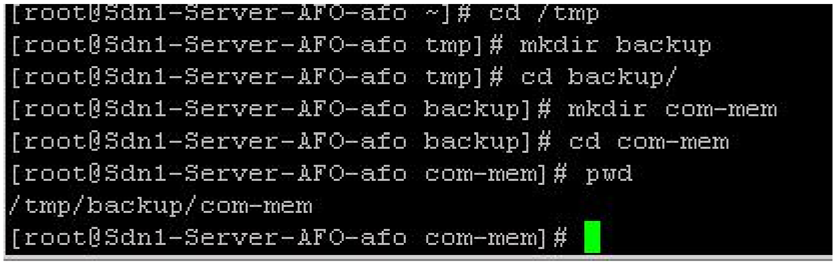
Before you begin

- You must successfully complete the backup of the legacy cluster.
- Ensure that you have reset the default password on the EFO web user interface.
- Ensure that you are able to launch EFO and you have added the EFO WebLM licenses.
- Ensure that you login as a root user on the EFO Management Server Console (MSC).

Procedure

1. Create the backup directory on the EFO MSC server.

   a. Create sub-folders for the respective applications under the newly created backup directory for data migration.

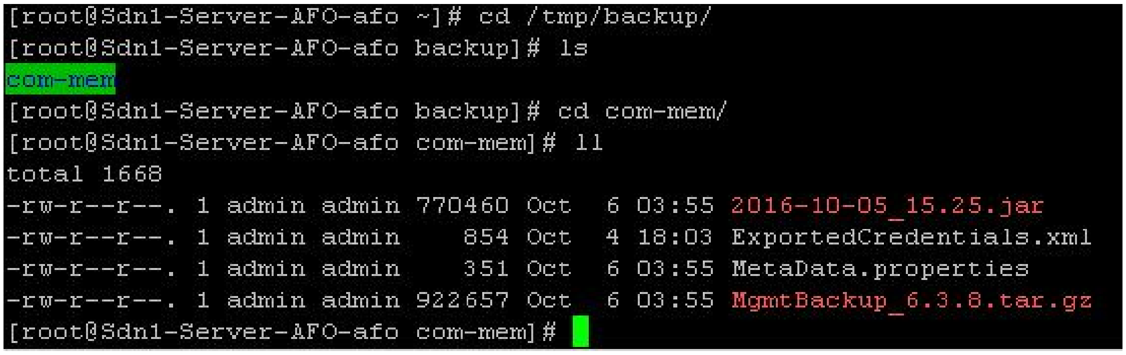


```
[root@Sdn1-Server-AFO-afo ~]# cd /tmp
[root@Sdn1-Server-AFO-afo tmp]# mkdir backup
[root@Sdn1-Server-AFO-afo tmp]# cd backup/
[root@Sdn1-Server-AFO-afo backup]# mkdir com-mem
[root@Sdn1-Server-AFO-afo backup]# cd com-mem
[root@Sdn1-Server-AFO-afo com-mem]# pwd
/tmp/backup/com-mem
[root@Sdn1-Server-AFO-afo com-mem]#
```

Example:

```
/tmp/backup/vpfm-mem
/tmp/backup/ipfm-mem
/tmp/backup/com-mem
```

b. Copy the backup files from the legacy cluster to their respective sub-folders.



```
[root@Sdn1-Server-AFO-afo ~]# cd /tmp/backup/
[root@Sdn1-Server-AFO-afo backup]# ls
com-mem
[root@Sdn1-Server-AFO-afo backup]# cd com-mem/
[root@Sdn1-Server-AFO-afo com-mem]# ll
total 1668
-rw-r--r--. 1 admin admin 770460 Oct  6 03:55 2016-10-05_15.25.jar
-rw-r--r--. 1 admin admin    854 Oct  4 18:03 ExportedCredentials.xml
-rw-r--r--. 1 admin admin    351 Oct  6 03:55 MetaData.properties
-rw-r--r--. 1 admin admin 922657 Oct  6 03:55 MgmtBackup_6.3.8.tar.gz
[root@Sdn1-Server-AFO-afo com-mem]#
```

c. **(Optional)** Export device credentials set from the legacy cluster (UCM or SMGR) to a local XML file and copy that file to the respective sub-folder along with the archives.

Note:

You need to rename the exported device credentials XML file in the format `ExportedCredentials.xml`.

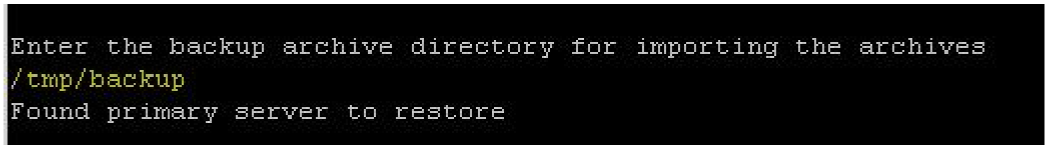
2. Login as a root user on the MSC server.
3. Run the following command:

   `/opt/avaya/smgr/dataMigration/DataMigration.sh`
4. Enter the EFO admin password to start the restore on EFO cluster.

   Note:

   You can restore the cluster back to the previous stable point in case a failure occurs during data migration.
5. Enter the backup directory path (exclude sub-folders) that you have created for importing the archives.

   The system displays the list of available applications to restore in an numbered list.



```
Enter the backup archive directory for importing the archives
/tmp/backup
Found primary server to restore
```

6. Enter the application number of the selected application to restore the data.

   The system displays the data migration summary of the selected application.
7. Enter `Y` to restore the archives mentioned in step 6. Otherwise, enter `N` to exit data migration.

Example

The following example depicts the data migration restore process.

- Login as a root user on MSC:.

  ```
  ******************** Starting data migration into AFO cluster *****************
  Enter the System manager login password:

  Backup of the current AFO setup is in progress, please wait...
  .................................
  Backup of the current AFO setup is complete
  ```

- Enter the backup archive directory path to copy the archive from the legacy cluster:

  ```
  /opt/avaya/archives
  ```

  Sample Output:

  ```
  Found back up data from the below primary servers, Please choose one of the below
  to restore session policies and jboss data.Users and roles information will be
  merged and migrated.

  1: flow-vm10.sv.avaya.com
  1

  Found back up data from the below flow servers, Please choose one of the below for
  restore.

  1: flow-vm10.sv.avaya.com
  1

  ------------------------------------------------------------------------------------
  -----------
  ```

- The sample output displays the data migration summary of the selected application:

  ```
  ------------------------------------------------------------------------------------
  -----------


  Data Migration Summary:


  Module         Archive                       Directory

  PLATFORM       2015-05-14_12.14.jar          /opt/avaya/smgr/dataMigration/manual/
  archives/RestoreDirectory/PRIMARY-SERVERS/Instance1

  FLOW           2015-05-14_12.14.jar          /opt/avaya/smgr/dataMigration/manual/
  archives/RestoreDirectory/MEMBER-SERVERS/IPFM-SERVERS/Instance1

  CONFIG

  MONITORING
  ```

Chapter 8: Getting started with EFO

Logging on to the web interface

About this task

Use this procedure to log on to the web interface for the first time.

Before you begin

Ensure that you have:

- Installed and configured the appliance.
- A computer with a supported web browser and access to the network where the appliance is installed.

Note:

Make sure that the FQDN is registered on your DNS server or add an entry in the hosts file of the machine that you use to access the system.

Procedure

1. On the web browser, enter `Platform/Monitoring/Configuration Server FQDN`.
2. In the **User ID** field, enter the default user name `admin`.
3. In the **Password** field, enter the default password `admin123`.
4. Click **Log On**.

   The system validates the user name and password with the user account. Depending on the validity, the system displays one of the following screens:

   - If the user name and password match, the system displays the web interface with the system `<version_number>`. The web interface displays the menu bar. The menu bar provides access to shared services to perform various operations that the system supports. The tasks that you can perform depend on your user role.
   - If the user name and password does not match, the system displays an error message and prompts you to re-enter the user name and password.

Next steps

- Change the default password.

Note:

You must change the password when you log on to the system using the default password for the first time.

The password must contain a combination of alphanumeric and special characters.

Changing the password

About this task

Use this procedure to change the default password for the web interface.

Important:

You must change the password when you log on to the system using the default password for the first time.

Before you begin

Ensure that you have:

- Installed and configured the appliance.
- A computer with a supported Internet Explorer, Firefox, or Safari web browser, and access to the network where the appliance is installed.

Procedure

1. On the web browser, enter `Platform/Monitoring/Configuration server FQDN`.
2. Click **Log On**.
3. In the **User ID** field, enter the user name.
4. In the **Current password** field, enter the current password.
5. In the **New password** field, enter the new password.
6. In the **Confirm new password** field, re-enter the new password.
7. Click **Save** to change the password.

Next steps

Install the system certificates.

Installing COM Plus and VPFM Plus certificates

About this task

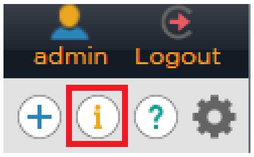
Perform this procedure to install COM Plus and VPFM Plus certificates using the web interface.

Before you begin

Ensure that you are logged into the Network Management web interface, using any one of the following supported browser:

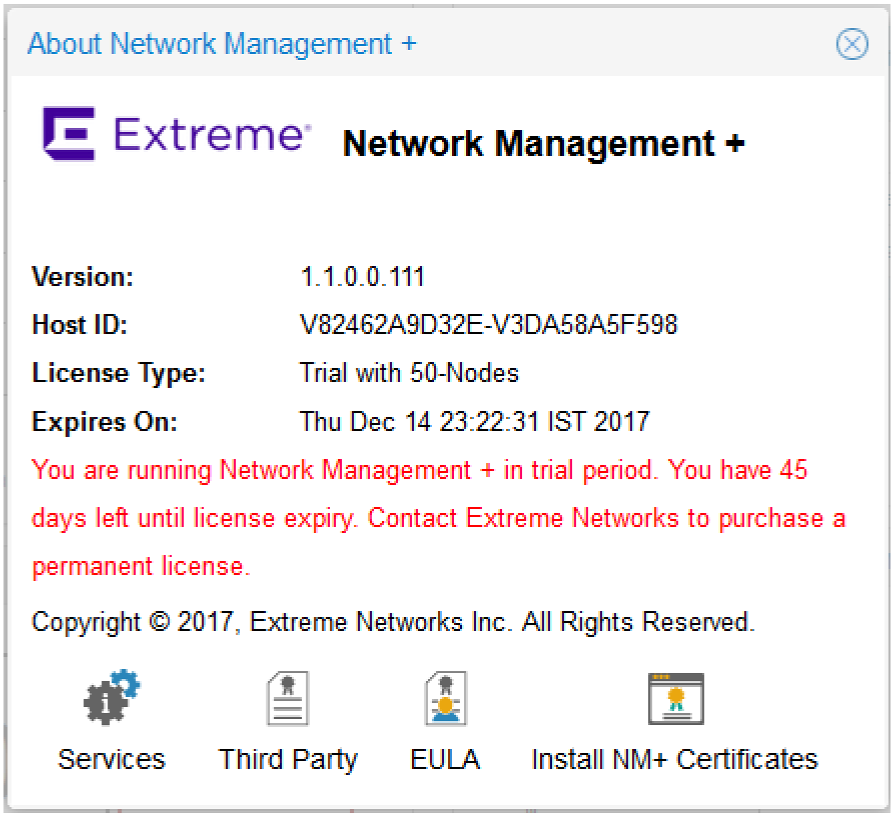
- Internet Explorer, version 11
- Mozilla Firefox, versions 54 and later
- Safari, versions MacOS v10.8 Mountain Lion and later

Procedure

1. 

   From the menu bar, click the icon from the quick access toolbar.

   The system displays the About Network Management + pop-up window.

   About Network Management +

   Extreme Network Management +

   Version: 1.1.0.0.111

   Host ID: V82462A9D32E-V3DA58A5F598

   License Type: Trial with 50-Nodes

   Expires On: Thu Dec 14 23:22:31 IST 2017

   You are running Network Management + in trial period. You have 45 days left until license expiry. Contact Extreme Networks to purchase a permanent license.

   Copyright © 2017, Extreme Networks Inc. All Rights Reserved.

   Figure 4: About Network Management + window

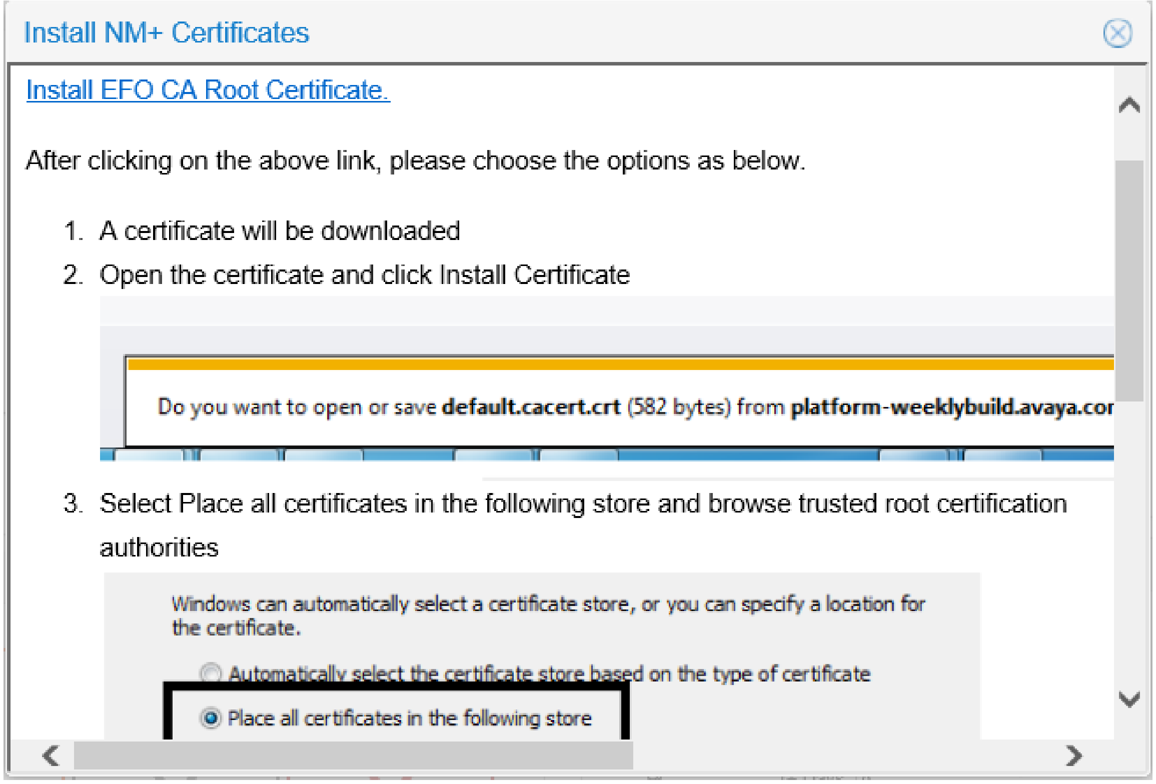
2. Click **Install NM+ Certificates** .

   The system displays the Install NM+ Certificates page.

   - The following image shows a sample of the Install NM+ Certificates page on an IE browser:

Note:

For IE browser, you must select the **Trusted Root Certification Authorities** store to install the certificate.



Install NM+ Certificates

Install EFO CA Root Certificate.

After clicking on the above link, please choose the options as below.

1. A certificate will be downloaded
2. Open the certificate and click Install Certificate

Do you want to open or save **default.cacert.crt** (582 bytes) from **platform-weeklybuild.avaya.cor**

3. Select Place all certificates in the following store and browse trusted root certification authorities

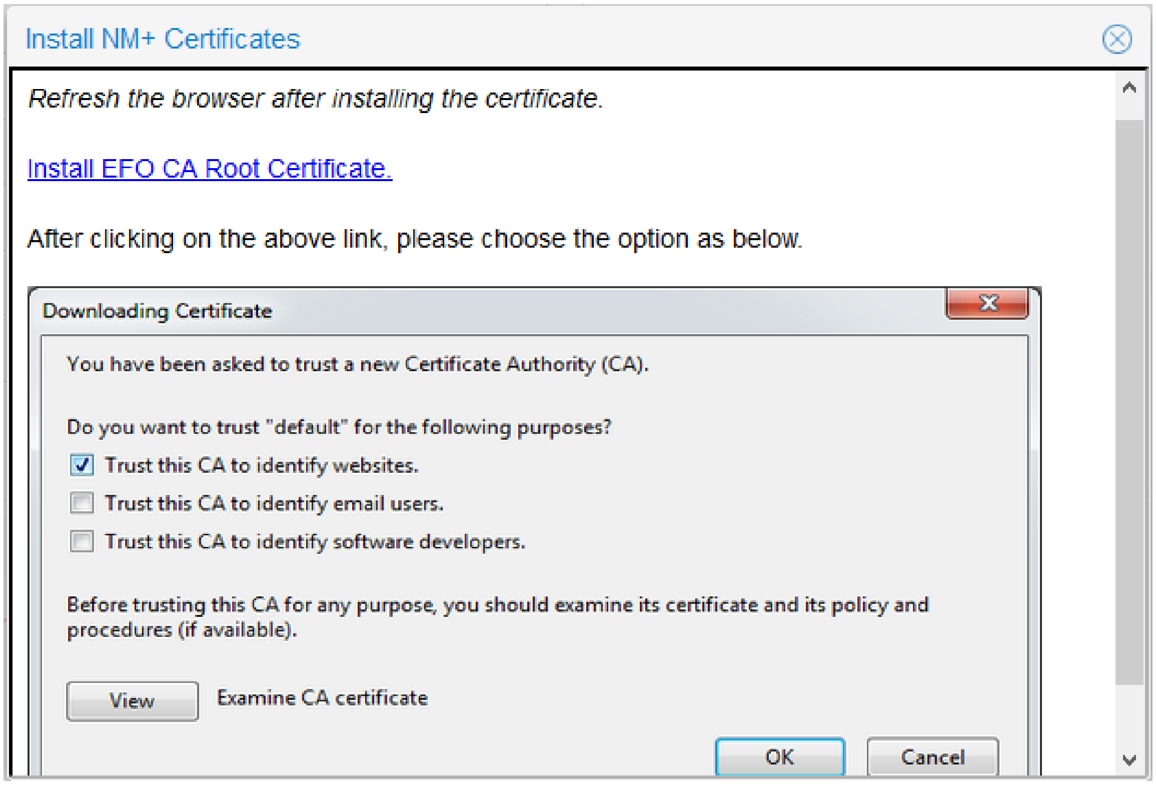
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Figure 5: Sample IE browser : Install NM+ Certificates

- The following image shows a sample of the Install NM+ Certificates page on a Mozilla Firefox browser:



Install NM+ Certificates

Refresh the browser after installing the certificate.

Install EFO CA Root Certificate.

After clicking on the above link, please choose the option as below.

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "default" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

Figure 6: Sample Mozilla Firefox browser: Install NM+ Certificates

3. Click **Install CA Root Certificate** and follow the instructions as given on your screen to install the certificate.
4. **Refresh** the web page to view the updated information.

Network Discovery

You must configure Network Discovery to run network auto-discoveries. A discovery is a snapshot taken of a part or a complete network. Select **Network** > **Discovery** to access the Network Discovery options.

You must complete the following steps after you log on to the system for the first time, and before you can browse your network.

- Configure device credentials using the Device and Server Credentials Editor available from **Administration** > **Credentials**.
- Select the Default discovery domain, or add a new discovery domain.
- Configure the discovery options for the discovery domain.
- Discover the domain.

Important:

A device must have SNMP credentials and be able to respond to SNMP for the system to add the device to the Device and Service Credentials Editor. If a device changes from Unmanaged to Managed by either adding credentials for the device or by enabling SNMP on the device after the discovery is completed, you must run rediscovery on the domain, or create a new domain to discovery the device.

On the Network Discovery page, you can work with discovery domains, configure discovery options, perform discoveries, and view discovery status.

Default discovery options

The system ships with a default domain. You cannot remove the domain or tab from Monitoring, but you can delete the content, seeds, and discovery data from this domain, and refine a new seed, and then run discovery. To access the options, go to **Network** > **Discovery**, and go to the options on the bottom left. The **Configuration** tab uses the domain information for network elements.

By default, the discovery has the following options:

- DNS Lookup (not selected)—Monitoring performs DNS lookup on all devices.
- Multi-vendor discovery (not selected)—Monitoring discovers devices from multiple third party vendors.
- Host Storage Discovery (not selected)—Monitoring discovers file systems based on Linux log-in and scan of file systems on a server.

The options above exist at the bottom left of the screen for **Network** > **Discovery**.

Chapter 9: Upgrade Solution

Upgrade overview and considerations

This chapter provides the process and procedures for upgrading Extreme Fabric Orchestrator (EFO) to Release 1.2.

Supported upgrade paths

The following table lists the supported options to upgrade to Extreme Fabric Orchestrator (EFO).

Current version	Upgrade using
Extreme Fabric Orchestrator (EFO) Rel 1.0 or 1.1	CLI, for more information see, Upgrade process on page 38.

Supported migration paths

Extreme Networks supports the platform, and application migration and upgrade from legacy applications. For information related to data migration from the supported legacy application versions to a newer version of Extreme Fabric Orchestrator (EFO), see Overview of Migration on page 23.

Pre-upgrade tasks and requirements

To successfully upgrade the EFO system to Release 1.2, you must complete all tasks and requirements as listed below.

Pre-upgrade tasks

The table contains the key tasks that are required to upgrade EFO to Release 1.2.

Task	Note
Ensure that you perform backup of your current release, using **`/opt/avaya/smgr/backuprestore/backupRestoreAFO.sh --backup`** command and save the backup on the remote server.	For more information, see Performing Backup for Release 1.0 or 1.1 on page 45.

Table continues…

Task	Note
Note: For Release 1.1 the backup filename is **`backupRestoreCluster.sh`**.	
Ensure that you perform backup of the WebLM license and save the copy on the remote server.	1. Log on to the EFO web user interface, as an administrator. 2. On the menu bar, click **Administration** > **Licenses**. The system displays the WebLM Home page. 3. In the product name table, select the product license to be exported. 4. Click **Export All Licenses**. The system exports the license file on the platform VM to the file path `/tmp/all_licenses.zip` . 5. Copy the `/tmp/all_licenses.zip` license file from the platform VM to the remote server.
Ensure that the maximum session time-out is set to 120 minutes.	1. Log on to the EFO web user interface, as an administrator. 2. On the menu bar, click **Administration** > **Policies** > **Session Properties**. 3. Enter **Maximum Session Time** and **Maximum Idle Time** to `120 minutes`.
Ensure that you are able to access the iLO Remote console.	1. Login to iLO, and verify if you can launch and use either of the .Net IRC or the Java IRC. For more information, read the enclosed *HP ProLiant DL360 Gen9 Server* setup overview information.

Pre-upgrade requirements

- Ensure that your system has the following hardware, supported browsers, and applications.

Hardware

- Minimum of two Ethernet cables (minimum of three for High Availability) for each appliance
- Monitor
- Keyboard

Applications

- **Base Operating System:**
  - RHEL 7.1, 64-Bit
- **Hypervisor:**
  - Redhat KVM version 7.1

	• **Virtual Network:** - OpenvSwitch bridge
Supported Browser	• Internet Explorer, version 11 • Mozilla Firefox, versions 54 and later • Safari, versions macOS v10.8 Mountain Lion, and later

Note:

Ensure that you connect a monitor to Hypervisor console (EFO server).

Upgrade Process

The following provides the upgrade sequence for upgrading to Release 1.2, that start with a system running Extreme Fabric Orchestrator (EFO) Release 1.0 or 1.1.

Upgrading a Standalone or Leader node EFO appliance to Release 1.2

About this task

Use this procedure to upgrade a Standalone or Leader node EFO appliance from Release 1.0 or 1.1 to Release 1.2.

Before you begin

- Ensure that the EFO dashboard is functioning and all the applications are running.
- Before upgrading a new or factory reset EFO appliance, login to the current web user interface as admin and configure a new admin password as prompted.
- Download the following upgrade bundles from PLDS to a client machine, and ensure the checksum matches:
  - EFO 1.2 Infrastructure and applications upgrade bundle
  - EFO 1.2 Upgrade Utility
- Run the EFO cluster backup and copy the backup files to a remote server location. See Performing Backup for Release 1.0 or 1.1 on page 45.
- Backup the WebLM license and copy to a remote server location. For more information, see *Administration using Extreme Fabric Orchestrator*, NN48100–600.
- For High Availability system configurations, ensure that the EFO VMs are running on the Leader node before initiating a system upgrade command.

Procedure

1. Use a SCP or SFTP client to transfer the upgrade bundles from your client machine to the EFO appliance KVM server `/opt/` folder as root user.

2. Use an iLO remote console or a direct server connection to login to KVM hypervisor as root user.

3. Enter the following commands to unzip the KVM upgrade CLI utility:

   ```
   #cd /opt
   #unzip KVM-UPG-CLI-UTILITY-<version>.zip
   ```

4. Enter the following commands to begin the upgrade from the KVM hypervisor:

   ```
   #cd /opt
   #bash upgradeSystem
   ```

   Caution:

   Do not press CTRL+C to terminate an upgrade in progress. Terminating an upgrade in progress can cause an unusable system state.

5. When prompted for the dashboard admin password, enter the EFO web user interface admin password and press enter.

   The upgrade process takes approximately 150 minutes to complete. You can track the upgrade process with the KVM hypervisor console connection. Do not close the console connection. Wait until the upgrade process completes.

   Important:

   Locking your PC while using the iLO console application can cause the EFO appliance to restart. Do not press CTRL+ALT+DEL to lock your client machine while using an iLO remote console window. You can lock your PC after you minimize the iLO console window and click on the desktop or another program.

   Note:

   For a High Availability system, the upgrade process transfers the upgrade files from the Standalone Leader node to the Standby Master node, and shuts down the Master node. After the Leader node upgrade process completes the system is running in Standalone mode. You must use following next steps to restore the HA license, and then perform a separate upgrade procedure on the Master node. For more information, see Upgrading a Standby Master node EFO appliance to Release 1.2 on page 40.

Next steps

1. Copy the WebLM license from the remote server to your computer.

   Note:

   Ensure to copy the license to the same computer that you are using to access the EFO web user interface.

2. Unzip the WebLM license file.
3. Login to the EFO web user interface using the existing system administrator credentials.
4. Navigate to the **Administration** > **Licenses** page.
5. Install the WebLM license file.
6. Navigate to the **Administration** > **Appliance Device Manager** page.

7. Select the **Monitoring VM** and click the **Restart Services** button.

Note:

Discovery and Monitoring services are unavailable while the kbmd service restarts.

Upgrading a Standby Master node EFO appliance to Release 1.2

About this task

Use this procedure to upgrade the Standby Master nodeEFO appliance from Release 1.1 to Release 1.2.

Before you begin

- Ensure you have completed the Leader node upgrade process and restored a HA license, see Upgrading a Standalone or Leader node EFO appliance to Release 1.2 on page 38.
- Ensure that the EFO VMs are running on the Leader node before initiating a Standby Master node system upgrade command.

Procedure

1. Use an iLO remote console or a direct server connection to login to the Standby Master node KVM hypervisor as root user.
2. Enter the following commands to begin the Master node upgrade from the KVM hypervisor:

   ```
   #cd /opt
   #bash upgradeSystem
   ```

   Caution:

   Do not press CTRL+C to terminate an upgrade in progress. Terminating an upgrade in progress can cause an unusable system state.

   The upgrade process takes approximately 60 minutes to complete. You can track the upgrade process with the KVM hypervisor console connection. Do not close the console connection. Wait until the upgrade process completes.

   Important:

   Locking your PC while using the iLO console application can cause the EFO appliance to restart. Do not press CTRL+ALT+DEL to lock your client machine while using an iLO remote console window. You can lock your PC after you minimize the iLO console window and click on the desktop or another program.
3. Once the upgrade process completes, login to the Standby Master node KVM hypervisor as root user and reboot the host to initiate the techless deployment installer script.
4. Use the deployment installer to join the Leader node, this procedure is the same as deploying a new High Availability system. See Deploying EFO High Availability on page 16.

Appendix A: IP addresses and ranges reference

This section provides details about the valid IP addresses and IP ranges used for device credentials.

✱ **Note:**

The current release of COM Plus and VPFM Plus supports IPv4 only. IPv6 is not supported.

Valid IP addresses and ranges

- IPv4 addresses must be in the same subnet range. IP addresses must be in the following format

  ```
  A.B.C.x-A.B.C.y (e.g,  192.0.2.0-192.0.2.24)
  ```

- Multiple IP Addresses must be separated by a comma (,). For example, the following are valid IPv4 addresses:

  ```
  [192.0.2.0-192.0.2.24] or [192.0.2.0-192.0.2.10, 192.0.2.16])
  ```

Appendix B: EFO server specifications

The following table lists the EFO server specifications.

Table 5: EFO server specifications

Quantity	Description
1	HP DL360 Gen9 4LFF CTO Server
1	755259-B21 HP DL360 Gen9 4LFF CTO Server
1	Opt. ABA U.S. - English localization
1	755394-L21 HP DL360 Gen9 E5-2680v3 FIO Kit
8	726719-B21 HP 16GB 2Rx4 PC4-2133P-R Kit
4	765424-B21 HP 600GB 12G SAS 15K 3.5in ENT SCC HDD
1	726536-B21 HP 9.5mm SATA DVD-ROM Jb Gen9 Kit
1	766211-B21 HP DL360 Gen9 LFF P440ar/H240ar SAS Cbl
1	749974-B21 HP Smart Array P440ar/2G FIO Controller
1	663202-B21 HP 1U LFF Ball Bearing Rail Kit
2	720478-B21 HP 500W FS Plat Ht Plg Pwr Supply Kit
1	663203-B21 HP 1U CMA for Ball Bearing Rail Kit
1	339779-B21 HP Raid 5 Drive 1 FIO Setting
1	H4396B HP No Additional Support Required
1	TA850AAE HP iLO Adv E-LTU inc 1yr TS&SW

Appendix C: Compatibility matrix for COM Plus and VPFM Plus 1.1

The following table lists the compatibility matrix for COM Plus and VPFM Plus 1.1.

Compatibility Matrix — Supported devices

Note:

For a complete list of supported devices, see *Network Management Supported Devices, Device MIBs, and Legacy Devices Reference*, NN48100–701.

Table 6: Supported devices

Device	Software releases
VOSS White-Box edition	4.3.1, 5.2, 5.3
Avaya Aura	7.0.1
Belden	6.0.2
Ethernet Routing Switch 1600	2.1.5.x, 2.1.6.x
Ethernet Routing Switch 2500	4.1.x, 4.2, 4.3, 4.4
Ethernet Routing Switch 3500	5.0, 5.0.1, 5.0.2, 5.1, 5.1.1, 5.1.3, 5.2, 5.2.3, 5.3, 5.3.1, 5.3.2
Ethernet Routing Switch 3600	6.0
Ethernet Routing Switch 4500	5.2 , 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2, 5.7, 5.7.2, 5.7.3
Ethernet Routing Switch 4800	5.2 , 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2, 5.7, 5.7.2, 5.7.3, 5.8, 5.8.2, 5.8.3, 5.9, 5.9.2. 5.9.5, 5.10
Ethernet Routing Switch 4900	7.1, 7.2, 7.3, 7.4, 7.4.1
Ethernet Routing Switch 5500	5.1, 6.0, 6.1, 6.2, 6.3, 6.6, 6.3.4, 6.3.5, 6.3.6, 6.6.1, 6.6.2, 6.6.3
Ethernet Routing Switch 5600	5.1, 6.0, 6.1, 6.2, 6.3, 6.6, 6.3.4, 6.3.5, 6.3.6, 6.6.1, 6.6.2, 6.6.3
Ethernet Routing Switch 5900	7.0, 7.0.1, 7.1, 7.2, 7.3. 7.4. 7.4.1
Ethernet Routing Switch 8600 & 8800 including the following hardware: 8681XLW module, 8681XLR module, 8616GTE module, 8672ATME MDA, 8608GBM module, 8608GTMmodule, 8632TXM	4.0, 4.1, 5.0, 5.1, 7.0, 7.1, 7.1.3, 7.1.5, 7.2, 7.2.10, 7.2.13, 7.2.14.x, 7.2.15

Table continues…

Device	Software releases
module, 8648TXM module, 8672ATMMmodule, 8683POSM module.	
Virtual Services Platform 4000	3.0, 3.0.1, 3.1, 4.0, 4.0.40, 4.0.50, 4.1, 4.2, 4.2.1, 4.2.2, 4.2.3, 4.5, 4.6, 5.0, 5.1, 5.1.1, 6.0, 6.1, 6.1.50
Virtual Services Platform 7000 (70XX)	10.1, 10.2, 10.2.1, 10.3, 10.3.1, 10.3.2, 10.3.3, 10.4
Virtual Services Platform 7200	4.2.1, 4.2.2, 4.2.3, 4.5, 4.6, 5.0, 5.1, 5.1.1, 5,3, 6.0, 6.1, 6.1.50
Virtual Services Platform 8000	4.0, 4.0.1.1, 4.1, 4.2, 4.2.1, 4.2.2, 4.2.3, 4.5, 4.6, 5.0, 5.1, 5.1.1, 5.3, 6.0, 6.1, 6.1.50
Virtual Services Platform 8600	4.5, 4.5.1
Virtual Services Platform 9000	3.0, 3.1, 3.2, 3.3, 3.4, 3.4.5.0, 4.0.1, 4.1, 4.1.1, 4.1.5
WLAN	23xx, AP 23xx
WLAN WC8100, AP8120	1.0, 1.1, 1.2

Appendix D: Performing Backup for Release 1.0 or 1.1

About this task

Use the following procedure to perform backup of EFO Release 1.0 or Release 1.1.

Before you begin

- Ensure that you are logged on to the MSC server.
- Enter `root username` and `password`.

Procedure

1. Login as a root user on the MSC server.
2. Run the backup command:

   For Release 1.0:

   ```
   /opt/avaya/smgr/backuprestore/backupRestoreAFO.sh --backup
   ```

   For Release 1.1:

   ```
   /opt/avaya/smgr/backuprestore/backupRestoreCluster.sh --backup
   ```
3. Enter password for the archive.
4. System validates the EFO cluster for backup procedure.
   - If validation is successful go to step 5.
   - Else, see the error message and rectify and go to step 1.
5. The system proceeds with a backup of EFO when the validation is successful.
6. The system displays the status of the backup and creates an archive at:`/opt/avaya/afo/shared/commonstorage/backups/`, if the status is `Successful`.

   Archive does not include backup of any add-ons deployed on the EFO cluster.

   Note:

   For Release 1.0. refer to the log file located at `/opt/avaya/smgr/log/AFOBackupRestore.log` for more details if the system `Failed` to take backup.

   For Release 1.1, refer to the log file located at `/opt/avaya/smgr/log/ClusterBackupRestore.log` for more details if the system `Failed` to take backup.