ExtremeCloud™ IQ Site Engine v26.11.10 High Availability Configuration Guide:

Failover Management and HA Setup

11/2026
26.11.10
PN: 9041351-00 Rev AA
Subject to Change Without Notice



Abstract

The High Availability Configuration Guide for ExtremeCloud IQ Site Engine version 26.11.10 provides detailed procedures for configuring and managing high availability (HA). Version 26.11.10 adds support for Hyper-V Failover Clustering as a supported HA configuration. You can configure HA from Microsoft Hyper-V 2025 with Windows Server Failover Clustering (WSFC) or using VMware vSphere 6.5 or 6.0. Leveraging HA, the system can automatically migrate and restart VMs in the event of hardware or software failure without manual intervention. The HA architecture uses host clusters for hardware redundancy, enabling seamless failover and minimizing service disruption. Configuration of HA includes continuous monitoring of server health, network isolation, and application failures with the Watchdog Service. The Hyper-V WSFC or vSphere HA application monitoring SDK automates VM resets upon failure detection. Comprehensive steps for setting up clusters, shared storage, and VM kernel network adapters are provided, as well as procedures for server upgrades while maintaining HA. Logging and diagnostic methods for both application monitoring and Watchdog services are also covered.

Copyright © 2026 Extreme Networks, Inc. All Rights Reserved.

Legal Notices

Extreme Networks, Inc., on behalf of or through its wholly-owned subsidiary, Enterasys Networks, Inc., reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

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

Contact

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

- **Global Technical Assistance Center (GTAC) for Immediate Support**
    - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or 1-603-952-5000. For the Extreme Networks 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.

Extreme Networks® Software License Agreement

This Extreme Networks Software License Agreement is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc. ("Extreme"), on behalf of itself and its Affiliates (as hereinafter defined and including its wholly owned subsidiary, Enterasys Networks, Inc. as well as its other subsidiaries). This Agreement sets forth Your rights and obligations with respect to the Licensed Software and Licensed Materials. BY INSTALLING THE LICENSE KEY FOR THE SOFTWARE ("License Key"), COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1. DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" shall refer to the License Key for software installed on one or more of Your servers. "Client Application" shall refer to the application to access the Server Application. "Licensed Materials" shall collectively refer to the licensed software (including the Server Application and Client Application), Firmware, media embodying the software, and the documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code imbedded in chips or other media. "Licensed Software" refers to the Software and Firmware collectively.
2. TERM. This Agreement is effective from the date on which You install the License Key, use the Licensed Software, or a Concurrent User accesses the Server Application. You may terminate the Agreement at any time by destroying the Licensed Materials, together with all copies, modifications and merged portions in any form. The Agreement and Your license to use the Licensed Materials will also terminate if You fail to comply with any term of condition herein.
3. GRANT OF SOFTWARE LICENSE. Extreme will grant You a non-transferable, non-exclusive license to use the machine-readable form of the Licensed Software and the accompanying documentation if You agree to the terms and conditions of this Agreement. You may install and use the Licensed Software as permitted by the license type purchased as described below in

License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4. LICENSE TYPES.
    - *Single User, Single Computer*. Under the terms of the Single User, Single Computer license, the license granted to You by Extreme when You install the License Key authorizes You to use the Licensed Software on any one, single computer only, or any replacement for that computer, for internal use only. A separate license, under a separate Software License Agreement, is required for any other computer on which You or another individual or employee intend to use the Licensed Software. A separate license under a separate Software License Agreement is also required if You wish to use a Client license (as described below).
    - *Client*. Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Software on your server and allow the specific number of Concurrent Users shown on the relevant invoice issued to You for each Concurrent User that You order from Extreme or Your dealer, if any, to access the Server Application. A separate license is required for each additional Concurrent User.
5. AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, You shall reimburse Extreme for all reasonable expenses related to such audit in addition to any other liabilities You may incur as a result of such non-compliance, including but not limited to additional fees for Concurrent Users over and above those specifically granted to You. From time to time, the Licensed Software will upload information about the Licensed Software and the associated devices to Extreme. This is to verify the Licensed Software is being used with a valid license. By using the Licensed Software, you consent to the transmission of this information. Under no circumstances, however, would Extreme employ any such measure to interfere with your normal and permitted operation of the Products, even in the event of a contractual dispute.
6. RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Software, or to translate the Licensed Software into another computer language.

    The media embodying the Licensed Software may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme's prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the

original media and all copies of the Licensed Software, in whole or in part, made by You. You may modify the machine-readable form of the Licensed Software for (1) your own internal use or (2) to merge the Licensed Software into other program material to form a modular work for your own use, provided that such work remains modular, but on termination of this Agreement, You are required to completely remove the Licensed Software from any such modular work. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7. TITLE AND PROPRIETARY RIGHTS

    a. The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

    b. You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8. PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme's exclusive property, and You shall use your best efforts (which in any event shall not be less than the efforts You take to ensure the confidentiality of your own proprietary and other confidential information) to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme's prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so.

    You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically

related to your use of the Licensed Software on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You agree to use your best efforts and take all reasonable steps to safeguard the Licensed Materials to ensure that no unauthorized personnel shall have access thereto and that no unauthorized copy, publication, disclosure, or distribution, in whole or in part, in any form shall be made, and You agree to notify Extreme of any unauthorized use thereof. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9. MAINTENANCE AND UPDATES. Updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide Software Updates, modifications, or enhancements, or Software maintenance and support services to You.
10. DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.
    a. Immediately after any termination of the Agreement or if You have for any reason discontinued use of Software, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Software from any modular works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme.
    b. Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.
11. EXPORT REQUIREMENTS. You are advised that the Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use.
12. UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13. LIMITED WARRANTY AND LIMITATION OF LIABILITY. The only warranty that Extreme makes to You in connection with this license of the Licensed Materials is that if the media on which the Licensed Software is recorded is defective, it will be replaced without charge, if Extreme in good faith determines that the media and proof of payment of the license fee are returned to Extreme or the dealer from whom it was obtained within ninety (90) days of the date of payment of the license fee.
NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. ONLY TO THE EXTENT SUCH EXCLUSION OF ANY IMPLIED WARRANTY IS NOT PERMITTED BY LAW, THE DURATION OF SUCH IMPLIED WARRANTY IS LIMITED TO THE DURATION OF THE LIMITED WARRANTY SET FORTH ABOVE. YOU ASSUME ALL RISK AS TO THE QUALITY, FUNCTION AND PERFORMANCE OF THE LICENSED MATERIALS. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.
Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14. JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

15. GENERAL.
    a. This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.
    b. This Agreement may not be changed or amended except in writing signed by both parties hereto.
    c. You represent that You have full right and/or authorization to enter into this Agreement.

d. This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme's assignees, licensors, and licensees.

e. Section headings are for convenience only and shall not be considered in the interpretation of this Agreement.

f. The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto.

g. Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

h. Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134 United States
ATTN: General Counsel

Table of Contents

ExtremeCloud™ IQ Site Engine v26.11.10High Availability Configuration Guide: 1

Failover Management and HA Setup 1

Abstract 2

Extreme Networks® Software License Agreement 4

Table of Contents 10

High Availability Support for ExtremeCloud IQ Site Engine with Hyper-V 2025 11

Introduction 11

Protecting Against Server Failure and Virtual Machine Isolation 11

Protecting Against Application Failure 12

Hardware Configuration 13

Configuring Hyper-V Failover Clustering 14

ExtremeCloud IQ Site Engine Upgrade Process 17

High Availability Support for ExtremeCloud IQ Site Engine with vSphere Version 6.5 18

Introduction 18

Protecting Against Server Failure and Virtual Machine Isolation 18

Protecting Against Application Failure 19

Hardware Configuration 20

Enabling vSphere HA 22

ExtremeCloud IQ Site Engine Upgrade Process 33

High Availability Support for ExtremeCloud IQ Site Engine with vSphere Version 6.0 36

Introduction 36

Protecting Against Server Failure and Virtual Machine Isolation 36

Protecting Against Application Failure 37

Hardware Configuration 38

Enabling vSphere HA 40

ExtremeCloud IQ Site Engine Upgrade Process 51

High Availability Support for ExtremeCloud IQ Site Engine with Hyper-V 2025

Introduction

While ExtremeCloud IQ Site Engine provides you with visibility into your entire network, there are circumstances that may result in ExtremeCloud IQ Site Engine becoming impaired or unresponsive. These include:

- The ExtremeCloud IQ Site Engine server becomes unresponsive or a virtual machine becomes isolated from the management network.
- Applications become unresponsive.
- A Hyper-V host fails due to a power or hardware failure.

The ExtremeCloud IQ Site Engine failover solution on Microsoft Hyper-V 2025 uses Windows Server Failover Clustering (WSFC), which provides a recovery plan in the event of a host power or hardware failure (such as a hard disk, memory, or CPU failure), an application failure, or if a virtual machine loses connectivity with the management network. With WSFC on Hyper-V 2025, you can monitor your ExtremeCloud IQ Site Engine servers, services, and applications. In addition, VMs can be reinitiated in the event of server and service failures without manual intervention.

Hyper-V with WSFC does not require user intervention or reliance on database backups, which can be hours or days old. Hyper-V with WSFC does not require a secondary ExtremeCloud IQ Site Engine server to be separately maintained and kept up-to-date, and does not rely on administrators or other networks that monitor for either the detection or recovery of host failures.

Hyper-V with WSFC falls under the Active/Cold-Standby category. Failover Clustering enables you to pool physical Hyper-V hosts into a logical group called a failover cluster. In a failover cluster, one instance of ExtremeCloud IQ Site Engine is deployed in the cluster. In the event of a failure to one Hyper-V host, this instance is live migrated to another available Hyper-V host in the cluster. The ExtremeCloud IQ Site Engine user interface typically takes about 10 minutes to restart.

NOTE: Hyper-V Failover Clustering is supported on Windows Server 2025. The ExtremeCloud IQ Site Engine VM must be configured on shared cluster storage and added to a failover cluster role.

Protecting Against Server Failure and Virtual Machine Isolation

ExtremeCloud IQ Site Engine's servers are organized into clusters on Hyper-V 2025. The cluster nodes running Hyper-V are monitored by the WSFC service. The WSFC service monitors the health of nodes in a cluster by sending heartbeat requests to each node. If a node does not respond within a configured

interval, the WSFC service identifies the failure and restarts the VM on a new node within the cluster. After the VM starts on another node, normal ExtremeCloud IQ Site Engine server operation resumes.

Hyper-V live migration also protects virtual machines against network isolation by migrating the VMs if the host becomes isolated on the management network, or loses connectivity on any of the management or data storage interfaces. Additionally, with the ExtremeCloud IQ Site Engine Hyper-V Failover Clustering solution the virtual machine is recovered on another node in the event that certain mission-critical services (such as database and server services) have stopped and not restarted under normal automated operating and recovery procedures.

Protecting Against Application Failure

ExtremeCloud IQ Site Engine uses a Watchdog Service (a Java process) to start the database, server processes, and services in the engine. If the database or server processes fail, the Watchdog Service monitors the status and restarts any that fail without the need for user intervention. Application monitoring resets the ExtremeCloud IQ Site Engine virtual machines based on health monitoring policies configured in the failover cluster role.

If the services fail to recover after multiple restarts, a VM restart might be the recommended solution. VM restart is not a function of the ExtremeCloud IQ Site Engine Watchdog Service. The Watchdog Service sends a heartbeat signal, and if a monitored service or process fails to recover after three service restarts, then the application might required a VM restart.

NOTE: If the watchdog service stops unexpectedly, application monitoring stops.

Logs for the Watchdog Service and application monitoring functionality can be found in the following locations:

- `<installation directory>/appdata/logs/watchdog.out` - Contains logs of starting/stopping watchdog process.
- `<installation directory>/appdata/logs/watchdog.log` - Contains runtime watchdog logs.
- `<installation directory>/appdata/logs/appmonitor.out` - Contains logs of starting/stopping app monitor.
- `<installation directory>/appdata/logs/appmonitor.log` - Contains runtime app monitor logs.

By default `appmonitor.log` and `watchdog.log` contain only informational logs. To get debug level logs, change the log4j configuration. To set the log level from info to debug for these logs:

1. Stop the Watchdog Service by entering `service nswatchdog stop` in the ExtremeCloud IQ Site Engine engine command line.

2. Navigate to the `<installation directory>/services/` directory. The properties files, watchdog.log4j.properties and appmonitor.log4j.properties contain the log configuration for watchdog service and Application monitor program respectively.
3. Open the `watchdog.log4j.properties` file and change **info** to **debug** in the following lines:
    - log4j.category.com.enterasys.netsight.watchdog=info
    - log4j.category.com.enterasys.netsight.watchdog.NetSightProcessController=info
    - log4j.category.com.enterasys.netsight.watchdog.NetSightDbProcessController=info
4. Open the `appmonitor.log4j.properties` file and change info to debug in the following lines:
    - log4j.category.com.enterasys.netsight.watchdog=info
    - log4j.category.com.enterasys.netsight.watchdog.VMGuestAppMonitor=info
5. Start the Watchdog Service by entering `service nswatchdog start` in the ExtremeCloud IQ Site Engine engine command line.

Hardware Configuration

A typical Hyper-V failover cluster configuration for ExtremeCloud IQ Site Engine consists of two or more Windows Server 2025 nodes with Hyper-V role enabled.

In this configuration, both Hyper-V hosts have the Hyper-V role installed and are configured as nodes in a Windows Server Failover Cluster. Both nodes share access to cluster-managed storage. Virtual machine disk (VHDX) files must be stored on shared storage that is accessible to all cluster nodes. The shared storage should be housed on a separate network to avoid network outages.

NOTE: The ExtremeCloud IQ Site Engine Failover Clustering solution requires that both hosts are configured as part of a Windows Server Failover Cluster, and have Hyper-V and Failover Clustering roles installed. All nodes, the cluster, and the ExtremeCloud IQ Site Engine VM must be in sync with the enterprise NTP server.

Failover Clustering monitors Hyper-V host availability and restarts failed VMs. Each node in the failover cluster communicates with a cluster heartbeat, which indicates if running as expected. If a heartbeat is not detected from any node within the cluster, the Failover Clustering service takes corrective action. If the VM fails, Failover Clustering attempts to restart the VM on the same node. If restart attempts are unsuccessful, the cluster can fail over the VM to another node. If the node fails, the VMs from that node are live-migrated to other nodes in the cluster.

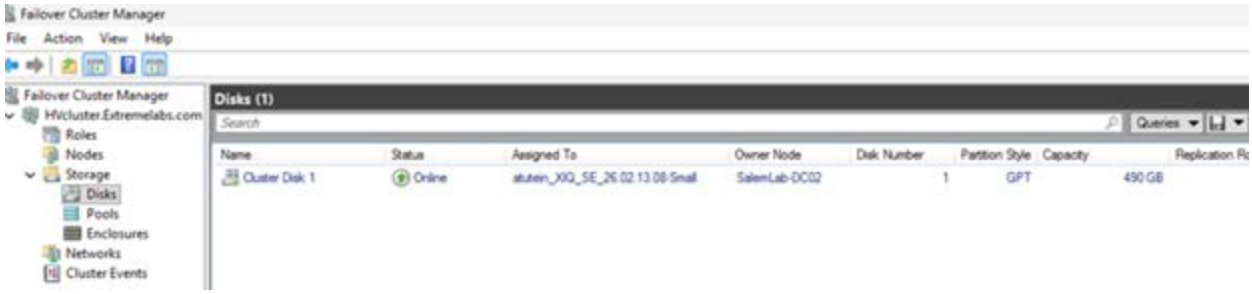
The shared cluster storage is the persistent storage for the virtual machine. It is where the ExtremeCloud IQ Site Engine server software is installed, the configuration information is kept, and where the database tables are stored. The virtual engine code is executed on the Hyper-V host. When a host fails, the virtual engine execution moves to the other host and all of the data is maintained in the

shared storage. This allows the ExtremeCloud IQ Site Engine server to continue functioning without having to restore a database backup.

Configuring Hyper-V Failover Clustering

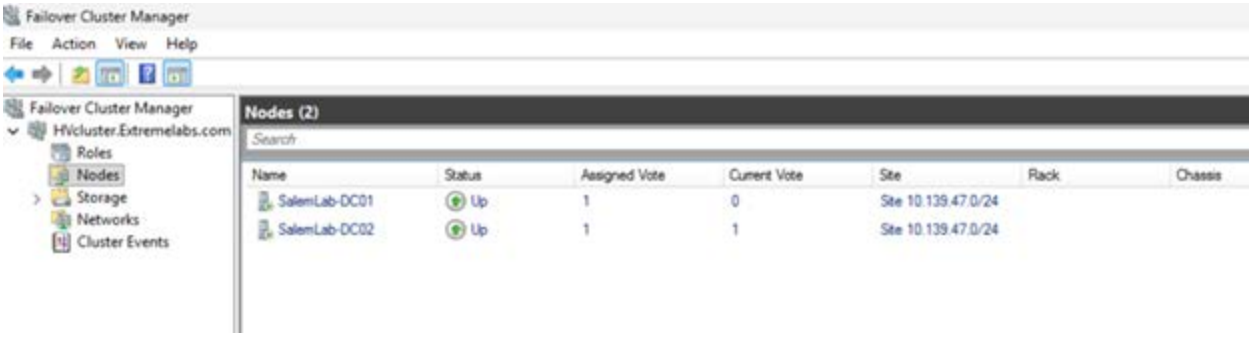
The following steps outline the process for setting up Windows Server Failover Clustering (WSFC) with Hyper-V 2025 for ExtremeCloud IQ Site Engine.

1. Prepare the Infrastructure:
    a. Install Windows Server 2025 on both cluster nodes.
    b. Install the Hyper-V role on both nodes.
    c. Install the Failover Clustering role on both nodes.
    d. Configure networking with redundant network adapters for cluster heartbeat traffic.
    e. Set up shared storage (iSCSI SAN, vSAN, or other shared storage solution) accessible to both nodes.
    f. Ensure all nodes have static IP addresses and are synchronized with an NTP server.
2. Create the Failover Cluster:
    a. Open **Failover Cluster Manager** on one of the cluster nodes.
    b. Select **Create Cluster** from the Actions pane.
    c. Follow the Create Cluster wizard to add both nodes.
    d. Configure cluster networks, quorum settings, and storage.
    e. Add the shared cluster storage as a cluster disk resource.

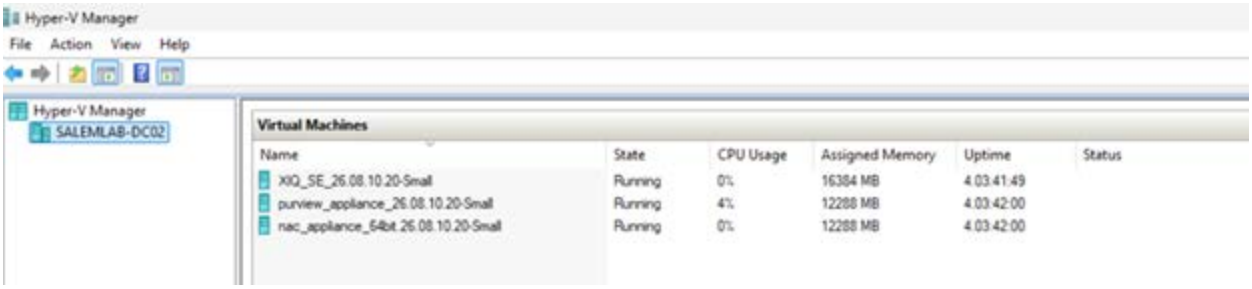


3. Configure the Shared Cluster Storage:
    a. Connect the shared storage (iSCSI, vSAN, or similar) to both Hyper-V hosts.
    b. Initialize and format the shared storage disk using Disk Management on both nodes.
    c. In Failover Cluster Manager, add the disk as a cluster resource.

    The shared storage will be used for virtual machine VHDX files and cluster-related data.



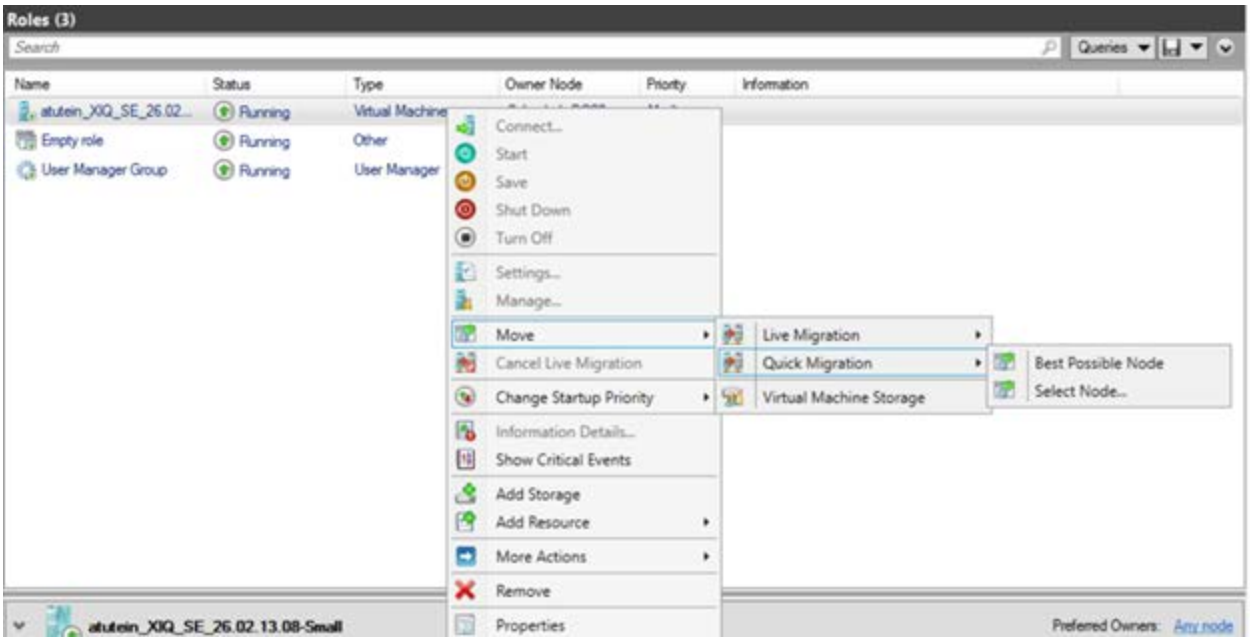
4. Create Virtual Machines on Shared Storage:
    a. From one of the Hyper-V hosts, open **Hyper-V Manager**.
    b. Create a new virtual machine for ExtremeCloud IQ Site Engine.
    c. Configure the VM to store its VHDX file on the shared cluster storage.
    d. Install ExtremeCloud IQ Site Engine on the VM.
    e. Repeat for additional appliances (Access Control Engine, Application Analytics Engine, etc.) if needed.



5. Add Virtual Machines to the Failover Cluster:
    a. Open **Failover Cluster Manager**.
    b. Navigate to Roles and select **Add a clustered role**.
    c. Select **Virtual Machine** as the role type.
    d. Select the ExtremeCloud IQ Site Engine VM to add to the cluster.
    e. Complete the wizard to add the VM as a cluster role resource
    f. Repeat for each appliance VM if running multiple appliances.



6. Configure the Failover and High Availability Settings:
    a. In Failover Cluster Manager, right-click the VM role and select Properties.
    b. Configure failover settings such as preferred node owners and failover thresholds.
    c. Configure the VM to automatically restart if it fails.
    d. Configure the health monitoring and recovery policies as needed.
    e. Apply the settings.
7. Test the Live Migration and Failover
    a. In Failover Cluster Manager, select the ExtremeCloud IQ Site Engine VM role.
    b. Right click and select **Move > Select Node** to initiate a live migration to another node.
    c. Monitor the live migration process. The VM should migrate with minimal service interruption.
    d. Test the automatic failover by intentionally failing a node or network connection. Observe the VM recovery.
    e. Verify that the ExtremeCloud IQ Site Engine services resume normally after a failover.



NOTE: For troubleshooting guidance, refer to the Microsoft documentation on Hyper-V and Windows Server Failover Clustering.

ExtremeCloud IQ Site Engine Upgrade Process

To upgrade an ExtremeCloud IQ Site Engine server on which Hyper-V Failover Clustering is currently configured, use the following instructions:

1. Open **Failover Cluster Manager**.
2. Select the cluster and navigate to **Roles**.
3. Right-click the ExtremeCloud IQ Site Engine VM role and select **Take Offline** to disable the failover protection during the upgrade.
4. Upgrade ExtremeCloud IQ Site Engine following the standard upgrade procedures.
5. After the upgrade is complete, return to **Failover Cluster Manager**.
6. Right-click the VM role and select **Bring Online** to enable Failover Clustering.

The ExtremeCloud IQ Site Engine user interface typically takes approximately 10 minutes to become available after the VM is brought online.

High Availability Support for ExtremeCloud IQ Site Engine with vSphere Version 6.0

High Availability Support for ExtremeCloud IQ Site Engine with vSphere Version 6.5

High Availability Support for ExtremeCloud IQ Site Engine with vSphere Version 6.5

Introduction

While ExtremeCloud IQ Site Engine provides you with visibility into your entire network, there are circumstances that may result in ExtremeCloud IQ Site Engine becoming impaired or unresponsive. These include:

- The ExtremeCloud IQ Site Engine server becomes unresponsive or a virtual machine becomes isolated from the management network.
- Applications become unresponsive.

ExtremeCloud IQ Site Engine's failover solution, the VMware vSphere High Availability (HA) feature, provides a recovery plan in the event of a host power or hardware failure (such as a hard disk, memory, or CPU failure), an application failure, or if a virtual machine loses connectivity with the management network. With vSphere HA, you can monitor your ExtremeCloud IQ Site Engine servers, services, and applications. In addition, VMs can be reinitiated in the event of server and service failures without manual intervention.

vSphere HA does not require user intervention or reliance on database backups, which can be hours or days old. It does not require a secondary ExtremeCloud IQ Site Engine server to be separately maintained and kept up-to-date, and it does not rely on administrators or other networks that monitor for either the detection or recovery of host failures.

vSphere HA falls under the Active/Cold-Standby category. vSphere HA enables you to pool physical servers into a logical group called an HA cluster. In vSphere HA, one instance of ExtremeCloud IQ Site Engine is deployed in the cluster on a host. In the event of a failure to the host, this instance is migrated and restarted across the available active ESXi hosts, depending on the type of failure. The ExtremeCloud IQ Site Engine user interface typically takes about 10 minutes to restart.

Protecting Against Server Failure and Virtual Machine Isolation

ExtremeCloud IQ Site Engine's servers are organized into clusters within the vCenter Server. The cluster servers running the vCenter Server software are called hosts. The vCenter Server monitors the health of hosts in a cluster by sending heartbeat requests to each host. If a host does not respond within a configured interval, the vCenter Server identifies that the host that failed and restarts the VM on a new host within the cluster. After the VM starts on another host, normal ExtremeCloud IQ Site Engine server operation resumes.

vSphere HA also protects virtual machines against network isolation by restarting the VMs if the host becomes isolated on the management network, or loses connectivity on any of the management or

data storage interfaces. Additionally, with the ExtremeCloud IQ Site Engine vSphere HA solution the virtual machine resets on the same host in the event that certain mission-critical services (such as database and server services) have stopped and not restarted under normal automated operating and recovery procedures.

Protecting Against Application Failure

ExtremeCloud IQ Site Engine uses a Watchdog Service (a Java process) to start database and/or server processes and services in the engine. Should the database and/or server processes fail, the Watchdog Service monitors their status and restarts any that fail without the need for user intervention. Application monitoring resets the ExtremeCloud IQ Site Engine virtual machines based on criteria defined in the **vSphere HA** > **VM Monitoring** options for the cluster. Modify the options for resetting during an application monitoring failure event to meet the needs of your network.

If the services fail to recover after multiple restarts, a VM restart might be the recommended solution. This is not a function of the ExtremeCloud IQ Site Engine Watchdog Service. vSphere HA includes an Application Monitoring SDK that performs VM resets if one or more heartbeats are missed.

The Watchdog Service sends an enable request to vSphere HA start the application monitoring, followed by a heartbeat signal. After the application monitoring is enabled and the Watchdog Service is initialized, the application monitoring status changes from gray to green. The application monitoring program continues to send the heartbeat and the status of the application monitoring remains green.

The vSphere infrastructure sends the signal from the HA application monitoring program to the VM, and then to the ESXi host. If a monitored service or process fails to recover even after three service restarts by the Watchdog Service, the application monitoring program stops sending the heartbeat. The status of application monitoring turns red if the heartbeat is not received in the first 30 seconds. After another 30 seconds, if the vSphere HA fails to receive another heartbeat, it activates the VM to reset.

This solution is a fully automated recovery process that provides protection against application failure by continuously monitoring VMs and resetting if failure is detected.

NOTES:
- vSphere HA application monitoring is limited to the Linux platform.
- vSphere HA application monitoring currently monitors Wildfly service and the MySQL DB service.

You can configure ExtremeCloud IQ Site Engine so the watchdog service so the Watchdog Service starts monitoring applications as part of the ExtremeCloud IQ Site Engine application initialization. When started, it continues to monitor and remedy the application service health.

NOTE: If the watchdog service stops unexpectedly, application monitoring stops.

Logs for the Watchdog Service and application monitoring functionality can be found in the following locations:

- `<installation directory>/appdata/logs/watchdog.out` - Contains logs of starting/stopping watchdog process.
- `<installation directory>/appdata/logs/watchdog.log` - Contains runtime watchdog logs.
- `<installation directory>/appdata/logs/appmonitor.out` - Contains logs of starting/stopping app monitor.
- `<installation directory>/appdata/logs/appmonitor.log` - Contains runtime app monitor logs.

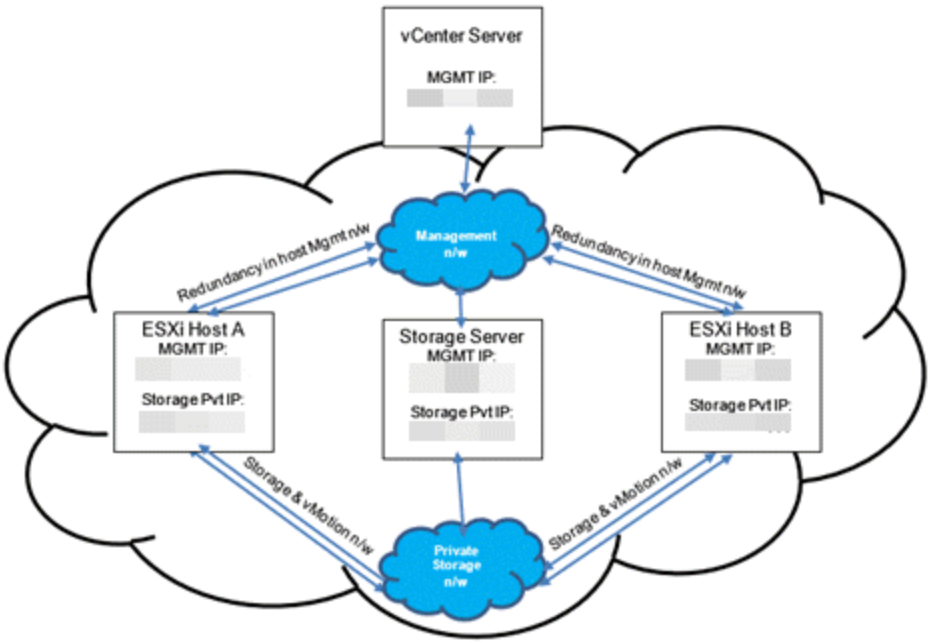
By default `appmonitor.log` and `watchdog.log` contain only informational logs. To get debug level logs, change the log4j configuration. To set the log level from info to debug for these logs:

1. Stop the Watchdog Service by entering `service nswatchdog stop` in the ExtremeCloud IQ Site Engine engine command line.
2. Navigate to the `<installation directory>/services/` directory. The properties files, watchdog.log4j.properties and appmonitor.log4j.properties contain the log configuration for watchdog service and Application monitor program respectively.
3. Open the `watchdog.log4j.properties` file and change **info** to **debug** in the following lines:
    - log4j.category.com.enterasys.netsight.watchdog=info
    - log4j.category.com.enterasys.netsight.watchdog.NetSightProcessController=info
    - log4j.category.com.enterasys.netsight.watchdog.NetSightDbProcessController=info
4. Open the `appmonitor.log4j.properties` file and change info to debug in the following lines:
    - log4j.category.com.enterasys.netsight.watchdog=info
    - log4j.category.com.enterasys.netsight.watchdog.VMGuestAppMonitor=info
5. Start the Watchdog Service by entering `service nswatchdog start` in the ExtremeCloud IQ Site Engine engine command line.

The vSphere HA feature also monitors the health of guest operating systems and their applications, and restarts the VM if a guest OS or application failure occurs. The vSphere HA feature monitors guest OS and application heartbeats via the VMware Tools process.

Hardware Configuration

The following diagram shows a typical hardware configuration for the ExtremeCloud IQ Site Engine Failover solution using vSphere's High Availability (HA) feature.



The vCenter Server is configured to manage two or more ESXi hosts in a cluster. In this configuration, there are two hosts with VMware's ESXi servers installed on them: Host A and Host B. Host A and Host B provide their servers redundancy by backing each other up in case of an outage or failure. Both hosts utilize the same data storage. VMDK (virtual machine disk) files must be stored on shared storage that is accessible to all servers. Also, the VMDK should be housed on a separate network to avoid network outage. vMotion networks are required within the vCenter Server clusters, and should use the same private storage network for quicker and seamless VM migrations.

NOTE: The ExtremeCloud IQ Site Engine Failover solution requires that vCenter Server is used to manage both hosts, and that the hosts are licensed for vSphere HA.

vCenter, the ESXi hosts, and the ExtremeCloud IQ Site Engine VM must be in sync with the enterprise NTP server.

vSphere HA monitors ESXi host availability and to restart failed VMs. Each host in the HA cluster communicates via a heartbeat, which indicates whether it is running as expected. If there's a failure to detect a heartbeat from any host within the cluster, vSphere HA is instructed to take corrective action. If the VM fails, vSphere HA attempts to restart the VM on the same host. If the host fails, the VMs from that host are migrated to other hosts in the cluster.

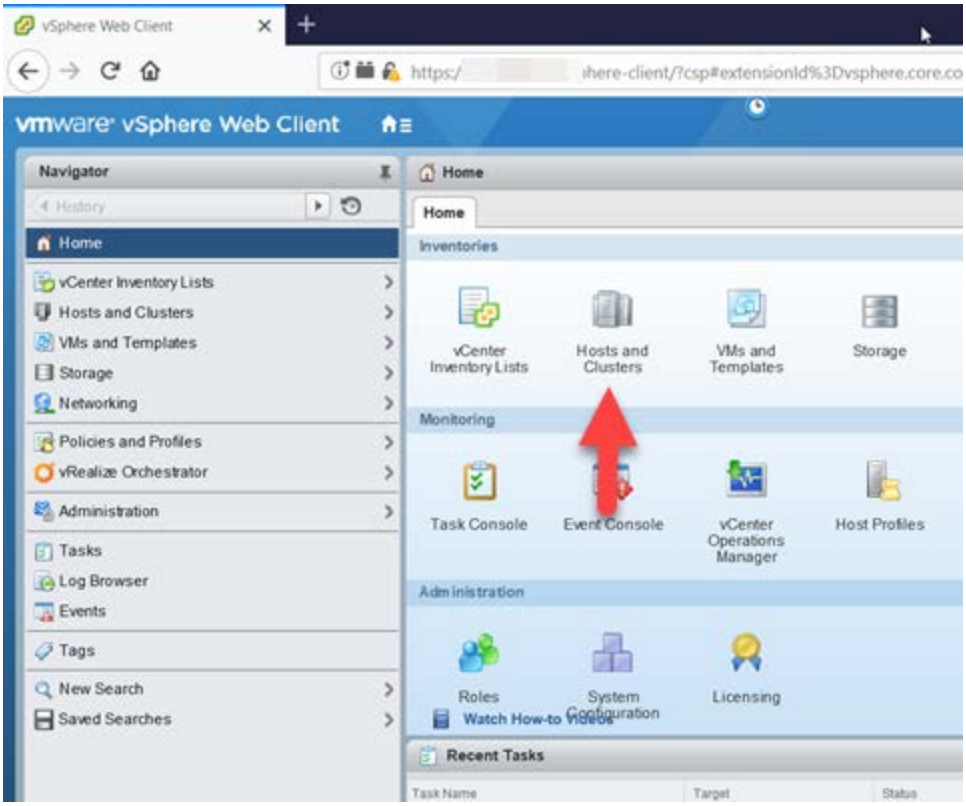
The datastore is the persistent storage for the virtual machine. It is where the ExtremeCloud IQ Site Engine server software is installed, the configuration information is kept, and where the database tables are stored. The virtual engine code is executed on the host. When a host fails, the virtual engine execution moves to the other host and all of the data is maintained in the datastore. This allows the ExtremeCloud IQ Site Engine server to continue functioning without having to restore a database backup.

NOTES: A Distributed Resource Scheduler (DRS) is often used with vSphere HA to redistribute workloads on alternate physical servers. A DRS is not required for vSphere HA.

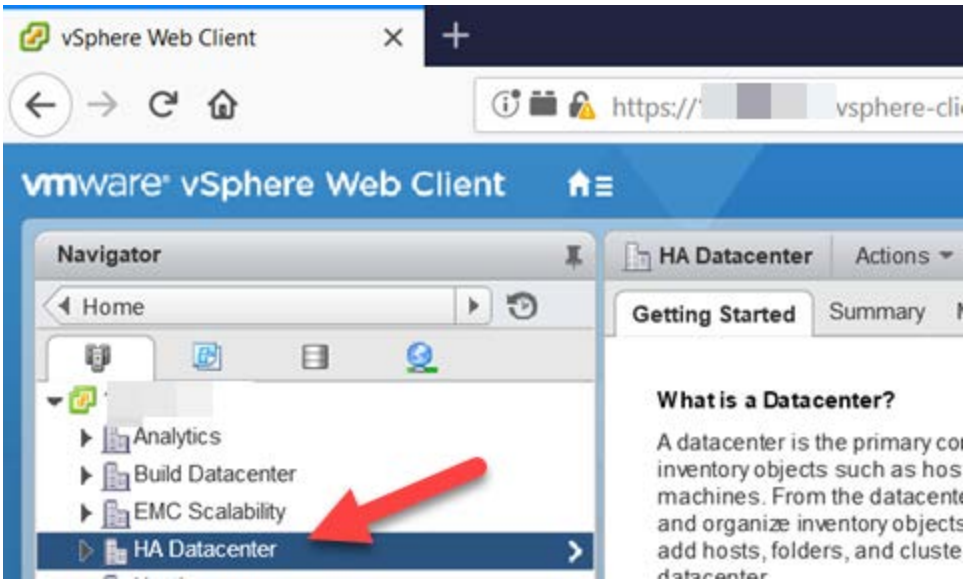
Enabling vSphere HA

When the licensed hosts are included in a cluster, you can enable vSphere HA using the cluster's settings in the New Cluster window. Refer to your VMware documentation for more information on configuring clusters.

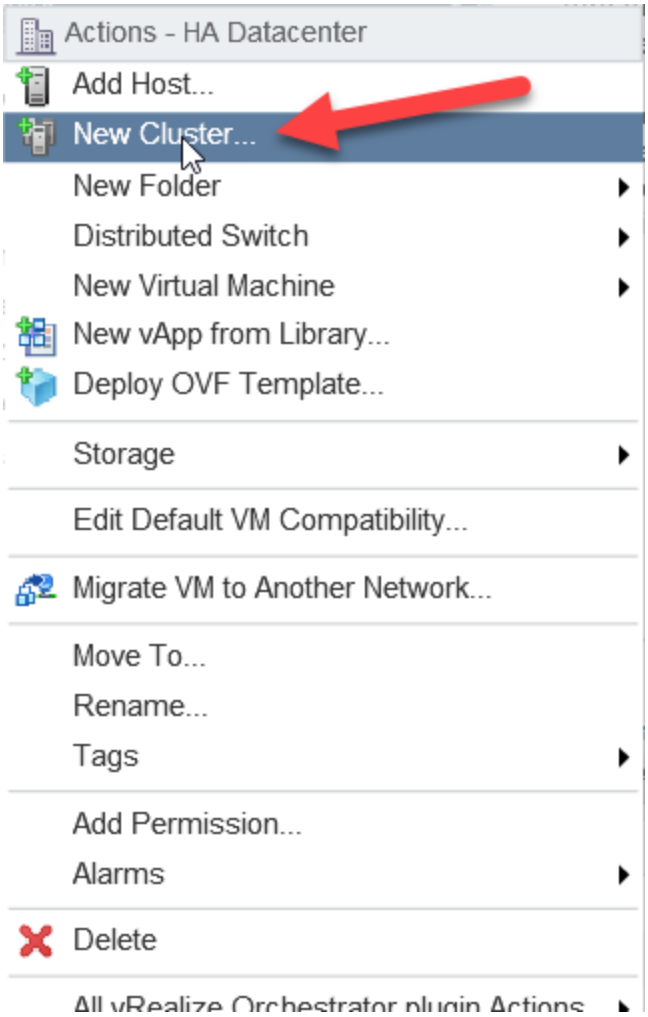
1. Log in to your vSphere Client.
2. Select **Hosts and Clusters** in the Inventories section.



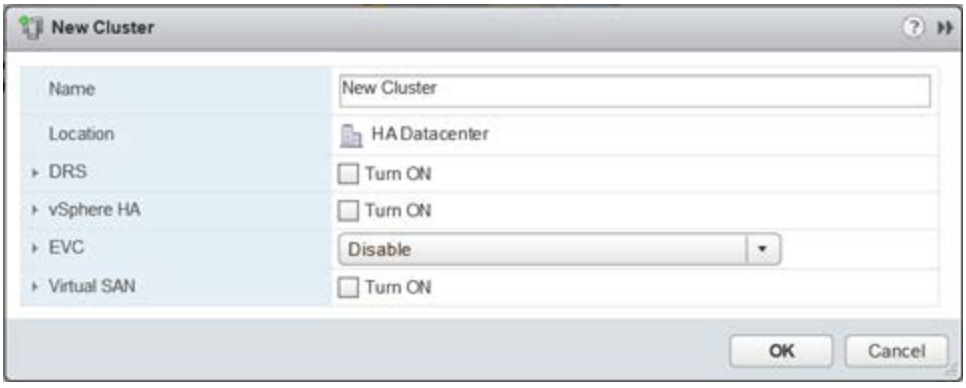
3. Select the datacenter in the left-panel on which you are adding the cluster.



4. Right-click the data center and select **New Cluster**.

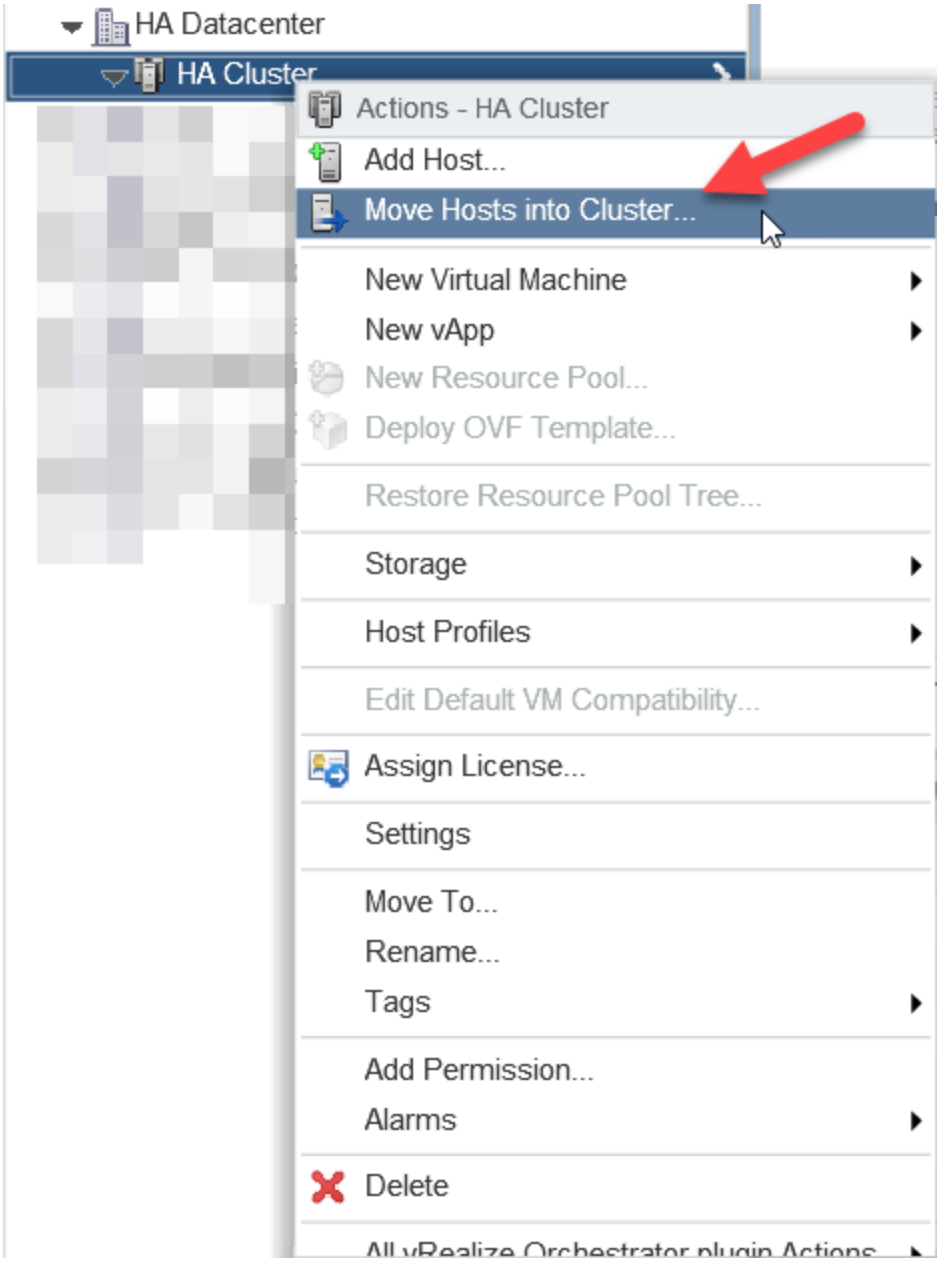


The **New Cluster** window displays.

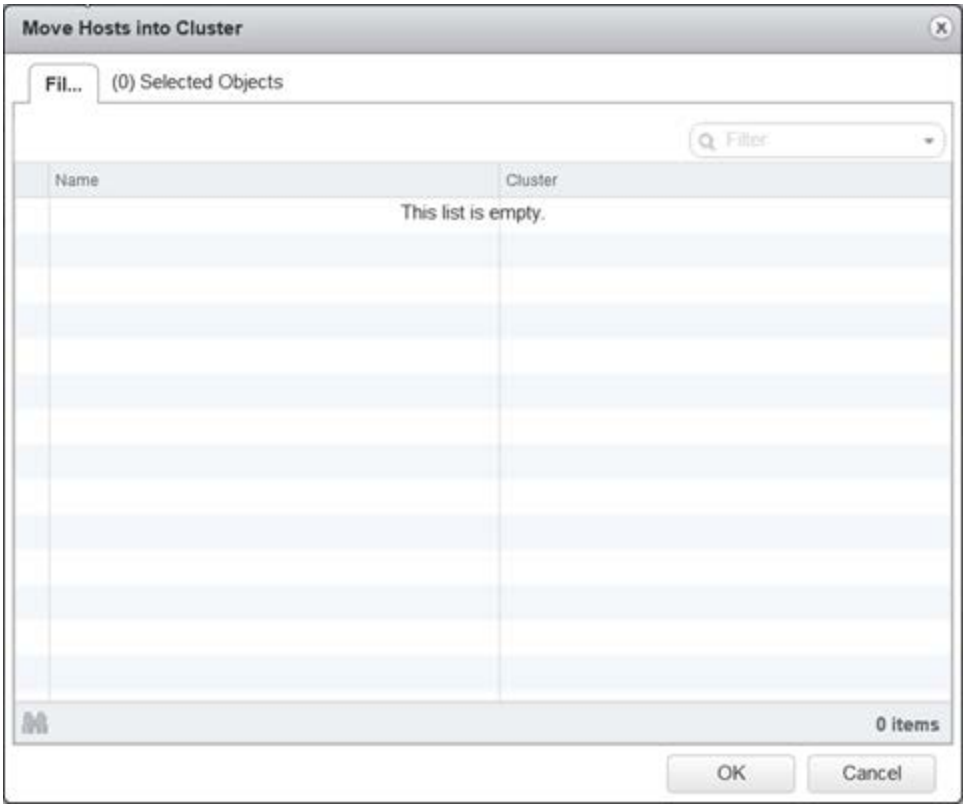


5. Configure the fields in the **New Cluster** window.
6. Select **vSphere HA** in the left-panel and select the box to enable.

7. Select **OK** to create an empty cluster.
8. Expand the datacenter in the left-panel so the cluster displays.
9. Right-click the cluster and select **Move Hosts into Cluster**.

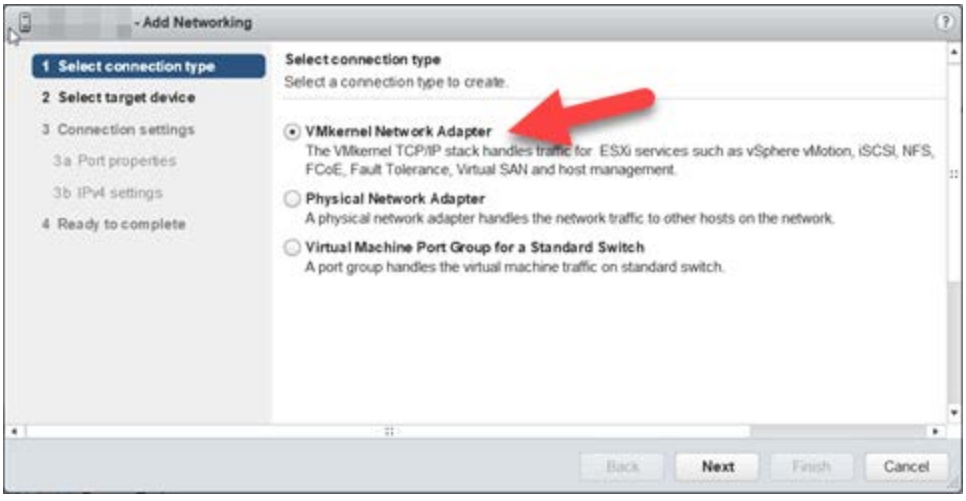


The **Move Hosts into Cluster** window displays.



10. Select the appropriate hosts to add to the cluster and select **OK**.
11. Expand the cluster in the left-panel.
12. Right-click a host from the left-panel and select **Add Networking**.

    The Add Networking wizard displays.



13. Select **VMkernal Network Adapter** and select **Next**.

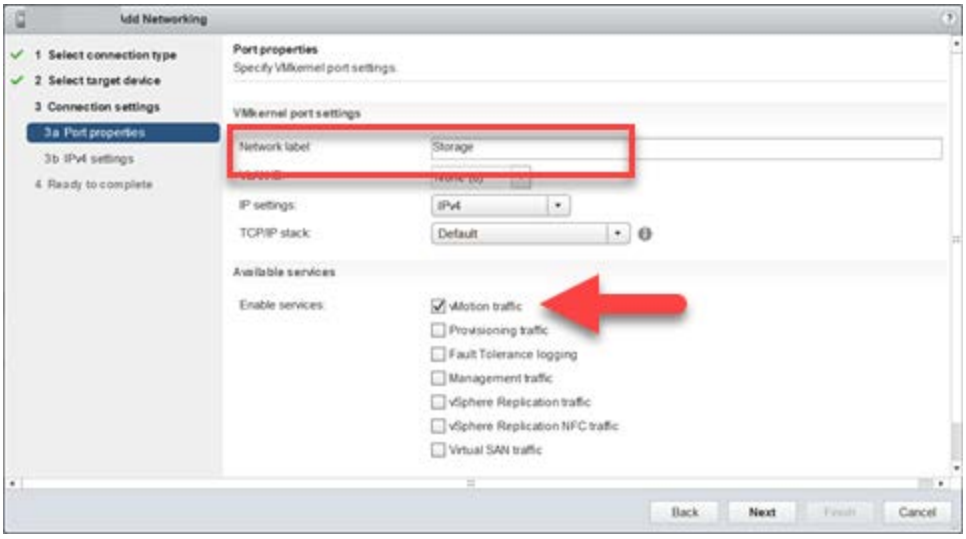
14. Select **Select an existing standard switch** radio button and select **Browse**.

    The **Select Switch** window displays.

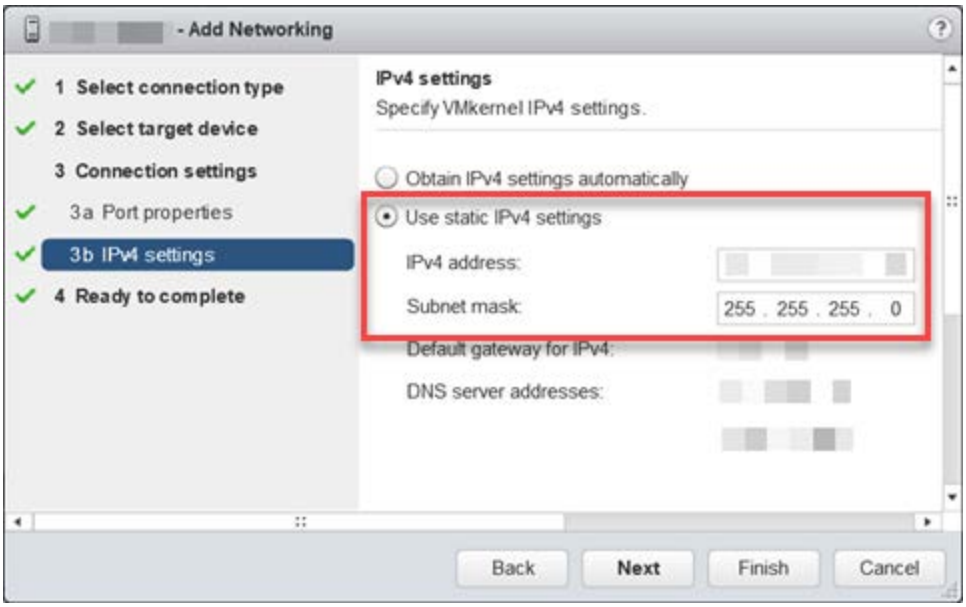
15. Select an unused existing vmnic from the list, select **OK**, and select **Next**.



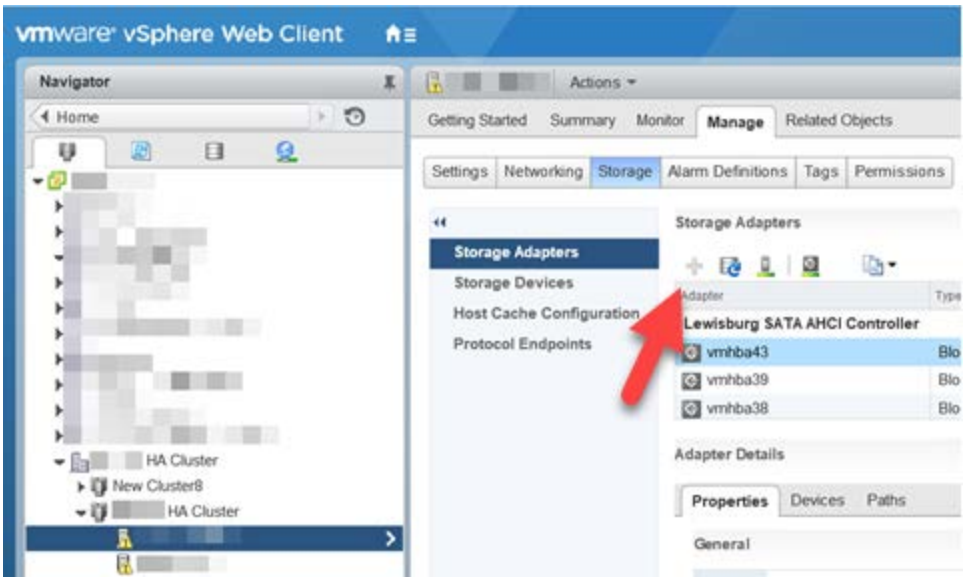
16. Enter **Storage** for Network label and select the **vMotion traffic** checkbox, then select **Next**.



17. Select **Use static IPv4** settings, enter the IP address for the storage server for the host being configured in the **IPv4 address** field, enter **255.255.255.0** in the **Subnet mask** field and select **Finish**.



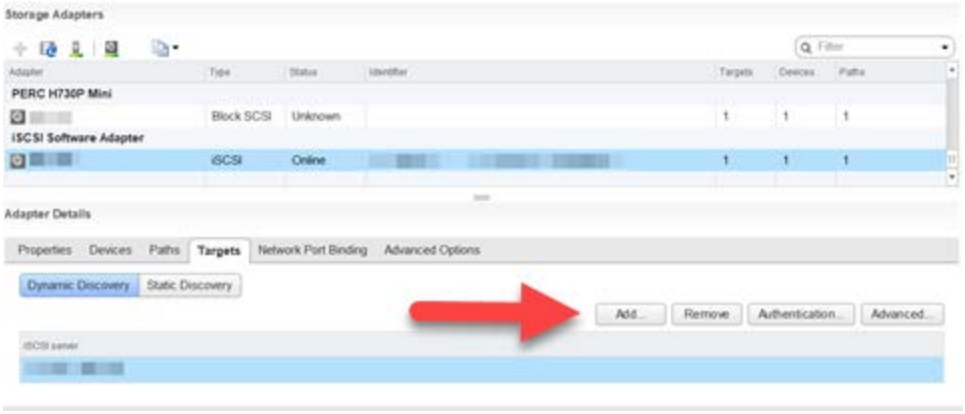
18. Repeat for all hosts in the cluster.
19. Select a host in the cluster in the left-panel and select the **Manage** tab.
20. Select **Storage**, **Storage Adapters**, and select the **Add** icon.



The adapter appears in the iSCSI Software Adapter section of the table.

21. Select the new adapter.
22. Select the **Targets** tab.

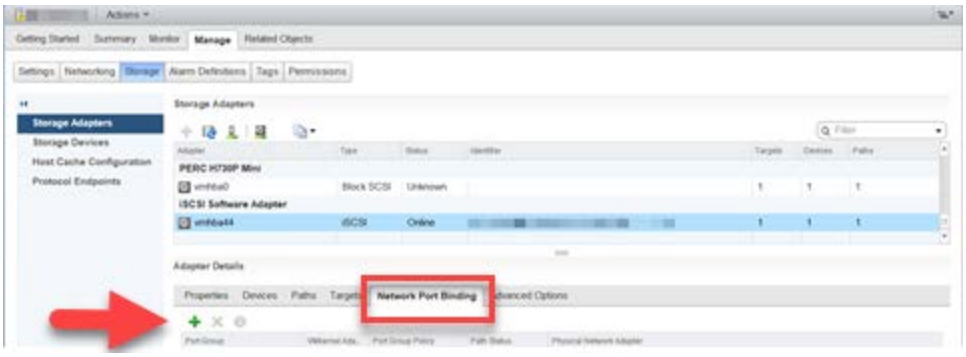
23. Select **Dynamic Discovery** and select **Add**.



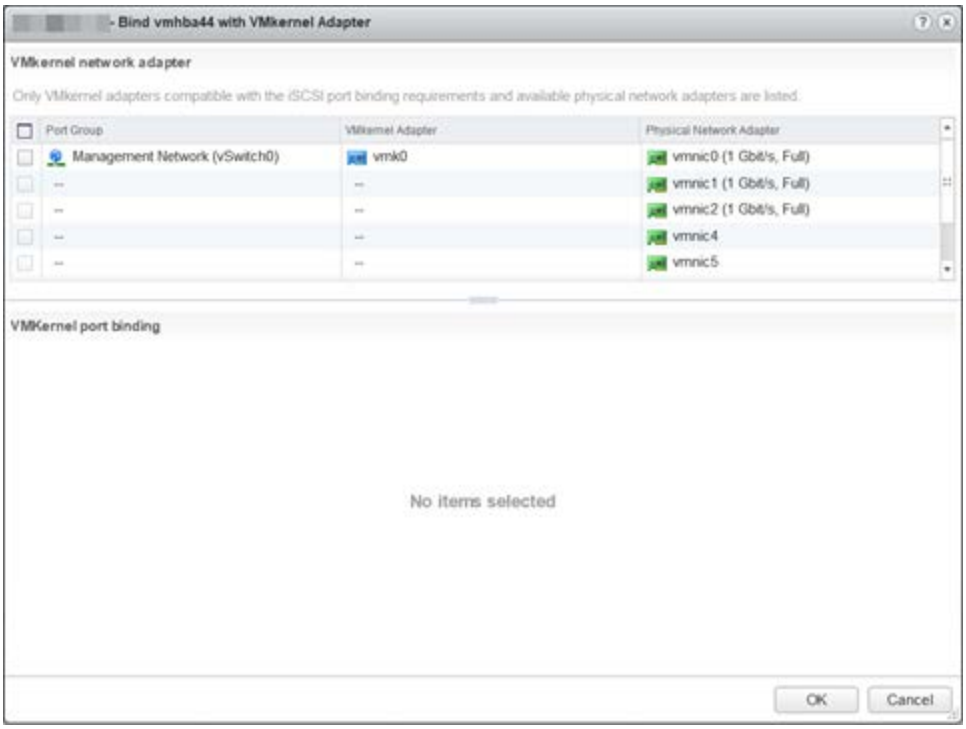
The **Add Send Target Server** window displays.



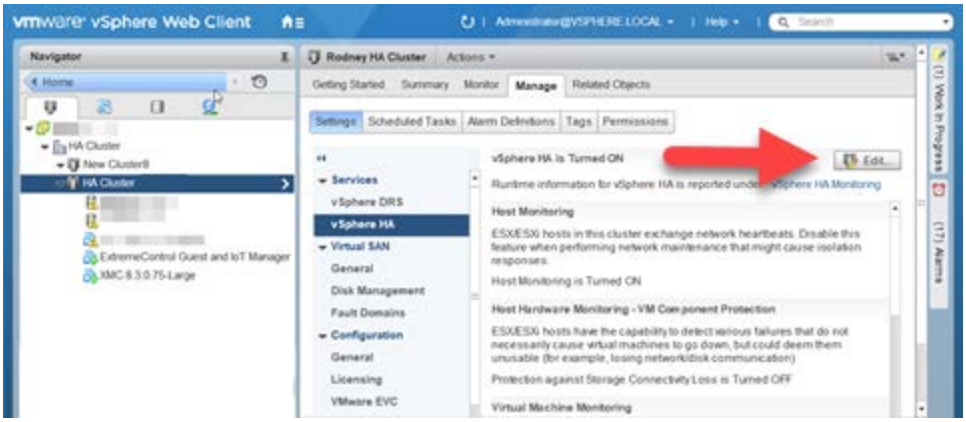
24. Enter the IP address of the storage server or full domain name in the **iSCSI Server** field and the port in the **Port** field.
25. Select **OK**.
26. Select the **Network Port Binding** tab and select the **Add** icon.



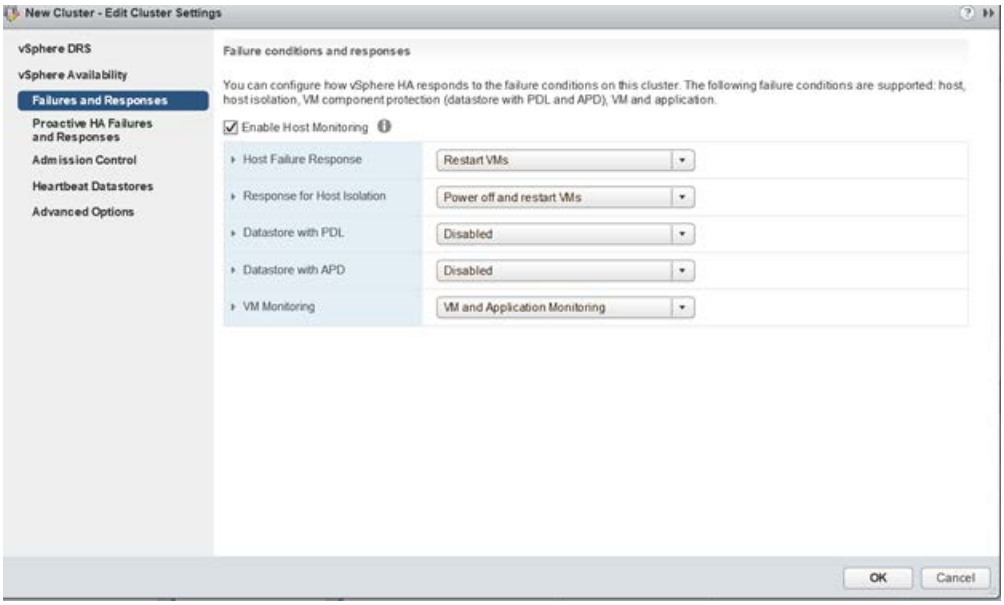
The **Bind with VMkernal Adapter** window displays.



27. Select the Storage created in Step 16.
28. Select the cluster you created in Step 6 in the left-panel.
29. Select the **Manage** tab in the right-panel and select **Settings**.
30. Select **vSphere HA** in the Services menu and select **Edit**.



The **Edit Cluster Settings** window displays.



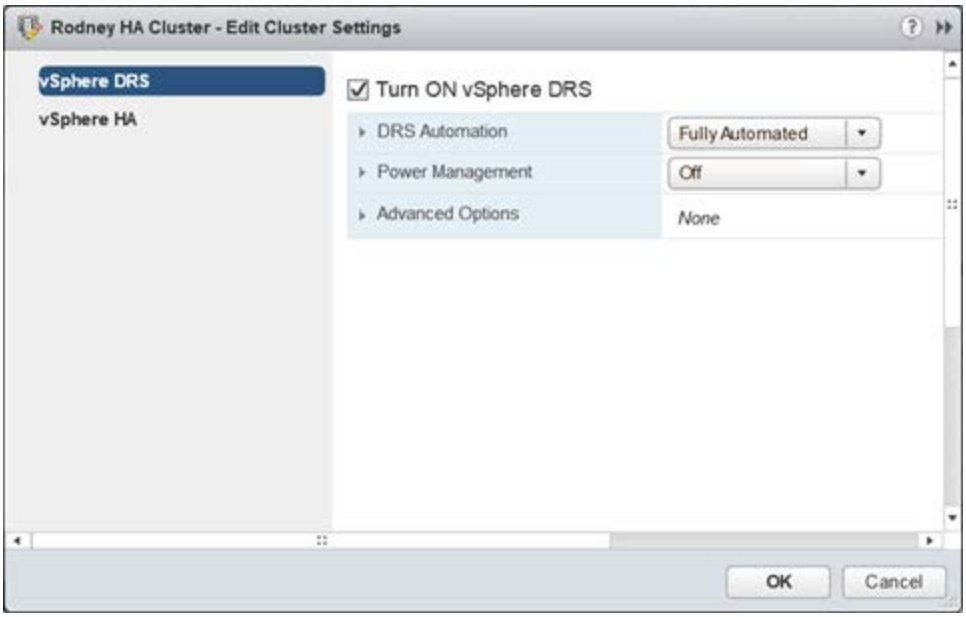
31. Select **Failures and Responses** in the left-panel.
32. Select the **Enable Host Monitoring** checkbox.
33. In the **Host Failure Response** drop-down list, select the action vSphere HA initiates if a host fails.
34. In the **Response for Host Isolation** drop-down list, select the action vSphere HA initiates if a host becomes isolated from the management network.

NOTE: Selecting **Leave Powered on** may cause impaired performance in ExtremeCloud IQ Site Engine or cause ExtremeCloud IQ Site Engine to become unresponsive.

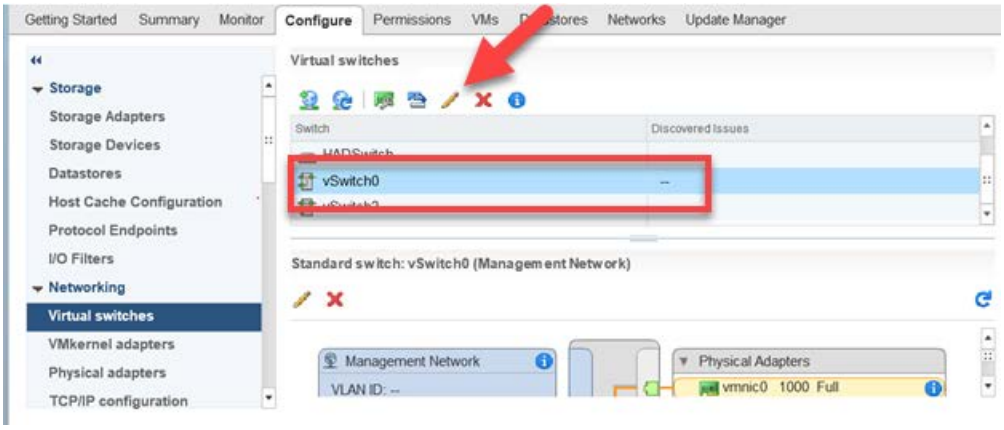
---

35. In the **VM Monitoring** drop-down list, select **VM Monitoring Only** or **VM and Application Monitoring**:
    - **VM Monitoring Only** — Virtual machines restart if vSphere does not receive the heartbeat within a certain amount of time.
    - **VM and Application Monitoring** — Enables ExtremeCloud IQ Site Engine monitoring via the Watchdog Service.
36. This is optional. In the **Datastore with PDL** and **Datastore with APD** drop-down lists, select a datastore to monitor hosts and virtual machines when the management network fails.

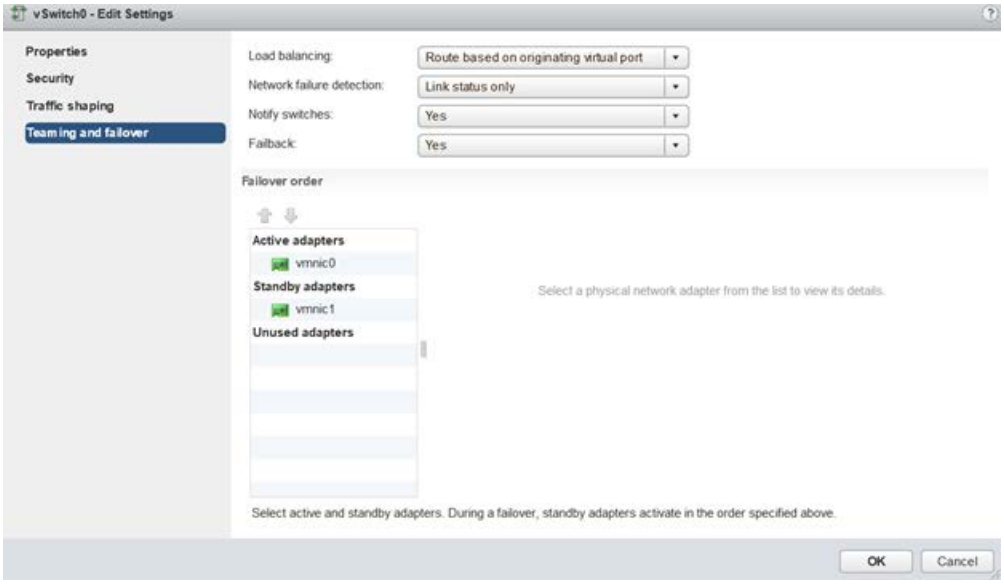
37. Select **vSphere DRS** in the left-panel of the window.



38. Select the **Turn ON vSphere DRS** checkbox.
39. Use the default values in the fields on this screen and select **OK**.
40. Additionally, you can create network redundancy on the host management network.
    a. Select the host, open the **Configure** tab, and select **Virtual switches** in the left-panel.
    b. In the Switch table in the right-panel, select the vSwitch on which you are configuring teaming and select the **Edit** icon.



The **Edit Settings** window displays.



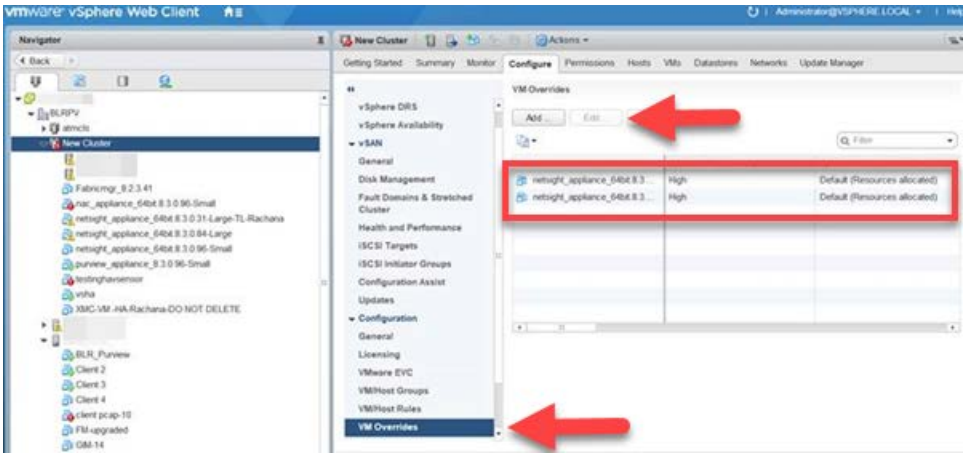
c. Select the appropriate teaming settings for the vSwitch.

d. Select **OK** to save.

ExtremeCloud IQ Site Engine Upgrade Process

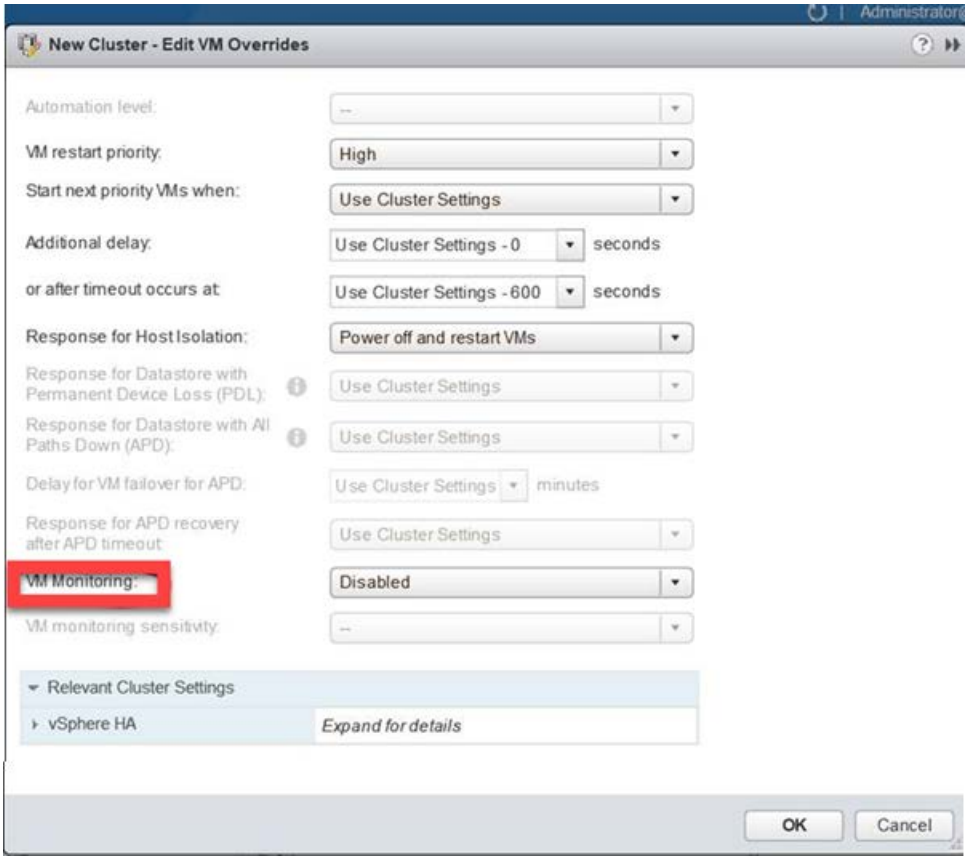
To upgrade an ExtremeCloud IQ Site Engine server on which VMware HA is currently configured, use the following instructions:

1. Log into your vSphere Client.
2. Select **Hosts and Clusters**.
3. Select the cluster on which HA is enabled.
4. Select the **Configure** tab in the right-panel and select **VM Overrides**.



5. Select the virtual machine for ExtremeCloud IQ Site Engine in the table and select **Edit**.

   The **Edit VM Overrides** window displays.



6. Select **Disabled** in the **VM Monitoring** drop-down list.
7. Select **OK**.
8. Upgrade ExtremeCloud IQ Site Engine.

9. Log into your vSphere Client.
10. Select **Hosts and Clusters**.
11. Select the cluster on which HA is enabled.
12. Select the **Configure** tab in the right-panel and select **VM Overrides**.
13. Select the virtual machine for ExtremeCloud IQ Site Engine in the table and select **Edit**.

    The **Edit VM Overrides** window displays.
14. Select **Enabled** in the **VM Monitoring** drop-down list.
15. Select OK.

High Availability Support for ExtremeCloud IQ Site Engine with vSphere Version 6.0

High Availability Support for ExtremeCloud IQ Site Engine with Hyper-V 2025

High Availability Support for ExtremeCloud IQ Site Engine with vSphere Version 6.0

Introduction

While ExtremeCloud IQ Site Engine provides you with visibility into your entire network, there are circumstances that may result in ExtremeCloud IQ Site Engine becoming impaired or unresponsive. These include:

- The ExtremeCloud IQ Site Engine server becomes unresponsive or a virtual machine becomes isolated from the management network.
- Applications become unresponsive.

ExtremeCloud IQ Site Engine's failover solution, the VMware vSphere High Availability (HA) feature, provides a recovery plan in the event of a host power or hardware failure (such as a hard disk, memory, or CPU failure), an application failure, or if a virtual machine loses connectivity with the management network. With vSphere HA, you can monitor your ExtremeCloud IQ Site Engine servers, services, and applications. In addition, VMs can be reinitiated in the event of server and service failures without manual intervention.

vSphere HA does not require user intervention or reliance on database backups, which can be hours or days old. It does not require a secondary ExtremeCloud IQ Site Engine server to be separately maintained and kept up-to-date, and it does not rely on administrators or other networks that monitor for either the detection or recovery of host failures.

vSphere HA falls under the Active/Cold-Standby category. vSphere HA enables you to pool physical servers into a logical group called an HA cluster. In vSphere HA, one instance of ExtremeCloud IQ Site Engine is deployed in the cluster on a host. In the event of a failure to the host, this instance is migrated and restarted across the available active ESXi hosts, depending on the type of failure. The ExtremeCloud IQ Site Engine user interface typically takes about 10 minutes to restart.

Protecting Against Server Failure and Virtual Machine Isolation

ExtremeCloud IQ Site Engine's servers are organized into clusters within the vCenter Server. The cluster servers running the vCenter Server software are called hosts. The vCenter Server monitors the health of hosts in a cluster by sending heartbeat requests to each host. If a host does not respond within a configured interval, the vCenter Server identifies that the host that failed and restarts the VM on a new host within the cluster. When the VM starts on another host, normal ExtremeCloud IQ Site Engine server operation resumes.

vSphere HA also protects virtual machines against network isolation by restarting the VMs if the host becomes isolated on the management network, or loses connectivity on any of the management or

data storage interfaces. Additionally, with the ExtremeCloud IQ Site Engine vSphere HA solution the virtual machine resets on the same host in the event that certain mission-critical services (such as database and server services) have stopped and not restarted under normal automated operating and recovery procedures.

Protecting Against Application Failure

ExtremeCloud IQ Site Engine uses a Watchdog Service (a Java process) to start database and/or server processes and services in the engine. Should the database and/or server processes fail, the Watchdog Service monitors their status and restarts any that fail without the need for user intervention. Application monitoring resets the ExtremeCloud IQ Site Engine virtual machines based on criteria defined in the **vSphere HA** > **VM Monitoring** options for the cluster. Modify the options for resetting during an application monitoring failure event to meet the needs of your network.

If the services fail to recover after multiple restarts, a VM restart might be the recommended solution. This is not a function of the ExtremeCloud IQ Site Engine Watchdog Service. vSphere HA includes an Application Monitoring SDK that performs VM resets if one or more heartbeats are missed.

The Watchdog Service sends an enable request to vSphere HA start the application monitoring, followed by a heartbeat signal. After the application monitoring is enabled and the Watchdog Service is initialized, the application monitoring status changes from gray to green. The application monitoring program continues to send the heartbeat and the status of the application monitoring remains green.

The vSphere infrastructure sends the signal from the HA application monitoring program to the VM, and then to the ESXi host. If a monitored service or process fails to recover even after three service restarts by the Watchdog Service, the application monitoring program stops sending the heartbeat. The status of application monitoring turns red if the heartbeat is not received in the first 30 seconds. After another 30 seconds, if the vSphere HA fails to receive another heartbeat, it activates the VM to reset.

This solution is a fully automated recovery process that provides protection against application failure by continuously monitoring VMs and resetting if failure is detected.

NOTES:
- vSphere HA application monitoring is limited to the Linux platform.
- vSphere HA application monitoring currently monitors Wildfly service and the MySQL DB service.

You can configure ExtremeCloud IQ Site Engine so the watchdog service so the Watchdog Service starts monitoring applications as part of the ExtremeCloud IQ Site Engine application initialization. When started, it continues to monitor and remedy the application service health.

NOTE: If the watchdog service stops unexpectedly, application monitoring stops.

Logs for the Watchdog Service and application monitoring functionality can be found in the following locations:

- `<installation directory>/appdata/logs/watchdog.out` - Contains logs of starting/stopping watchdog process.
- `<installation directory>/appdata/logs/watchdog.log` - Contains runtime watchdog logs.
- `<installation directory>/appdata/logs/appmonitor.out` - Contains logs of starting/stopping app monitor.
- `<installation directory>/appdata/logs/appmonitor.log` - Contains runtime app monitor logs.

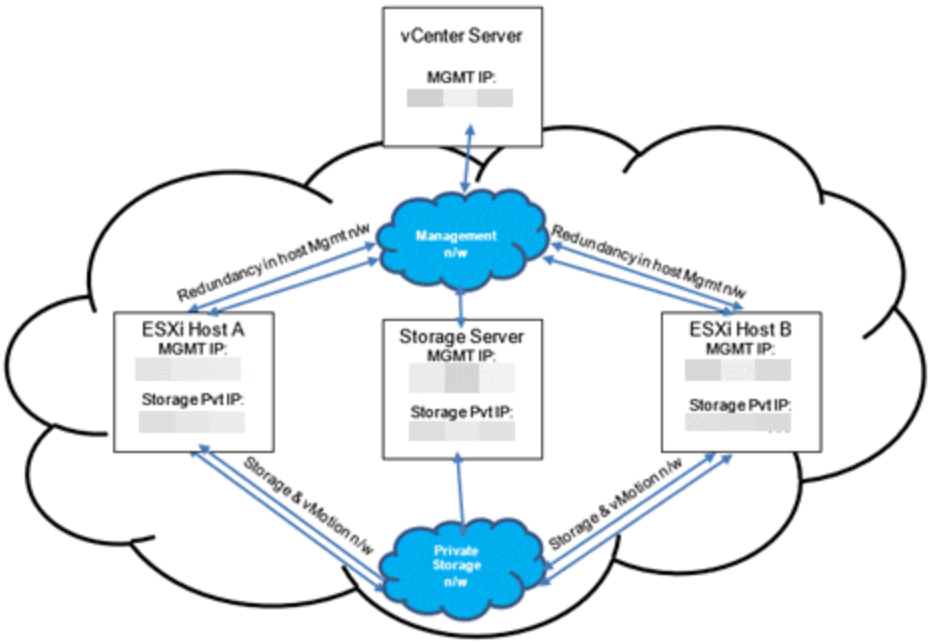
By default `appmonitor.log` and `watchdog.log` contain only informational logs. To get debug level logs, change the log4j configuration. To set the log level from info to debug for these logs:

1. Stop the Watchdog Service by entering `service nswatchdog stop` in the ExtremeCloud IQ Site Engine engine command line.
2. Navigate to the `<installation directory>/services/` directory. The properties files, watchdog.log4j.properties and appmonitor.log4j.properties contain the log configuration for watchdog service and Application monitor program respectively.
3. Open the `watchdog.log4j.properties` file and change **info** to **debug** in the following lines:
    - log4j.category.com.enterasys.netsight.watchdog=info
    - log4j.category.com.enterasys.netsight.watchdog.NetSightProcessController=info
    - log4j.category.com.enterasys.netsight.watchdog.NetSightDbProcessController=info
4. Open the `appmonitor.log4j.properties` file and change info to debug in the following lines:
    - log4j.category.com.enterasys.netsight.watchdog=info
    - log4j.category.com.enterasys.netsight.watchdog.VMGuestAppMonitor=info
5. Start the Watchdog Service by entering `service nswatchdog start` in the ExtremeCloud IQ Site Engine engine command line.

The vSphere HA feature also monitors the health of guest operating systems and their applications, and restarts the VM if a guest OS or application failure occurs. The vSphere HA feature monitors guest OS and application heartbeats via the VMware Tools process.

Hardware Configuration

The following diagram shows a typical hardware configuration for the ExtremeCloud IQ Site Engine Failover solution using vSphere's High Availability (HA) feature.



The vCenter Server is configured to manage two or more ESXi hosts in a cluster. In this configuration, there are two hosts with VMware's ESXi servers installed on them: Host A and Host B. Host A and Host B provide their servers redundancy by backing each other up in case of an outage or failure. Both hosts utilize the same data storage. VMDK (virtual machine disk) files must be stored on shared storage that is accessible to all servers. Also, the VMDK should be housed on a separate network to avoid network outage. vMotion networks are required within the vCenter Server clusters, and should use the same private storage network for quicker and seamless VM migrations.

NOTE: The ExtremeCloud IQ Site Engine Failover solution requires that vCenter Server is used to manage both hosts, and that the hosts are licensed for vSphere HA.

vCenter, the ESXi hosts, and the ExtremeCloud IQ Site Engine VM must be in sync with the enterprise NTP server.

vSphere HA monitors ESXi host availability and to restart failed VMs. Each host in the HA cluster communicates via a heartbeat, which indicates whether it is running as expected. If there's a failure to detect a heartbeat from any host within the cluster, vSphere HA is instructed to take corrective action. If the VM fails, vSphere HA attempts to restart the VM on the same host. If the host fails, the VMs from that host are migrated to other hosts in the cluster.

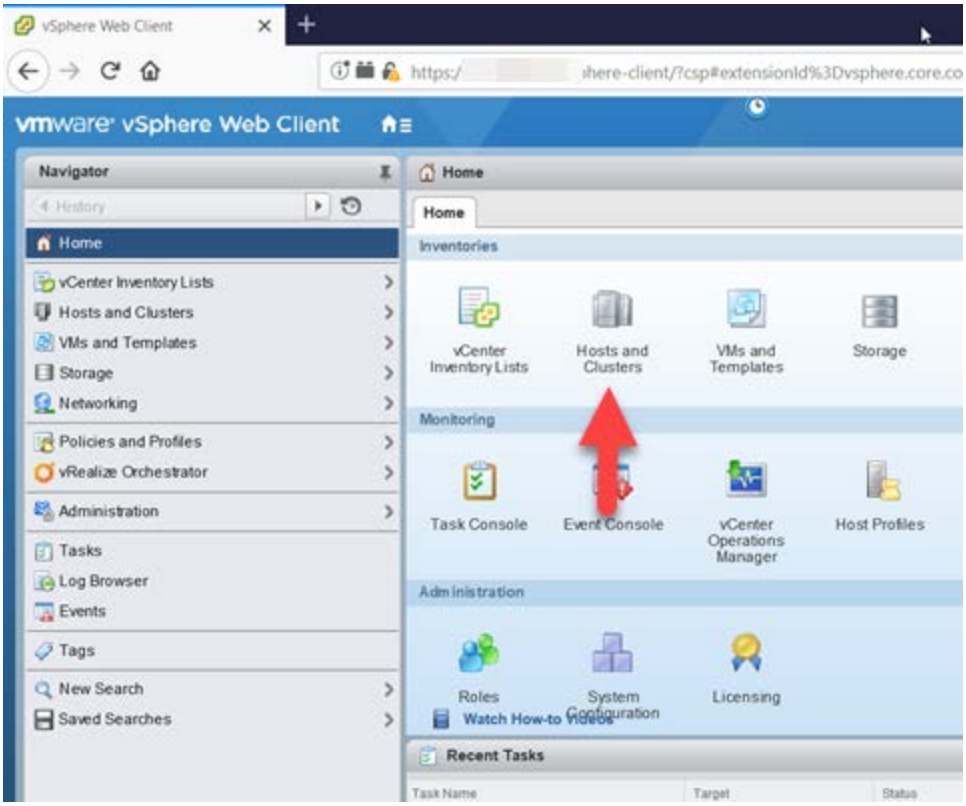
The datastore is the persistent storage for the virtual machine. It is where the ExtremeCloud IQ Site Engine server software is installed, the configuration information is kept, and where the database tables are stored. The virtual engine code is executed on the host. When a host fails, the virtual engine execution moves to the other host and all of the data is maintained in the datastore. This allows the ExtremeCloud IQ Site Engine server to continue functioning without having to restore a database backup.

NOTES: A Distributed Resource Scheduler (DRS) is often used with vSphere HA to redistribute workloads on alternate physical servers. A DRS is not required for vSphere HA.

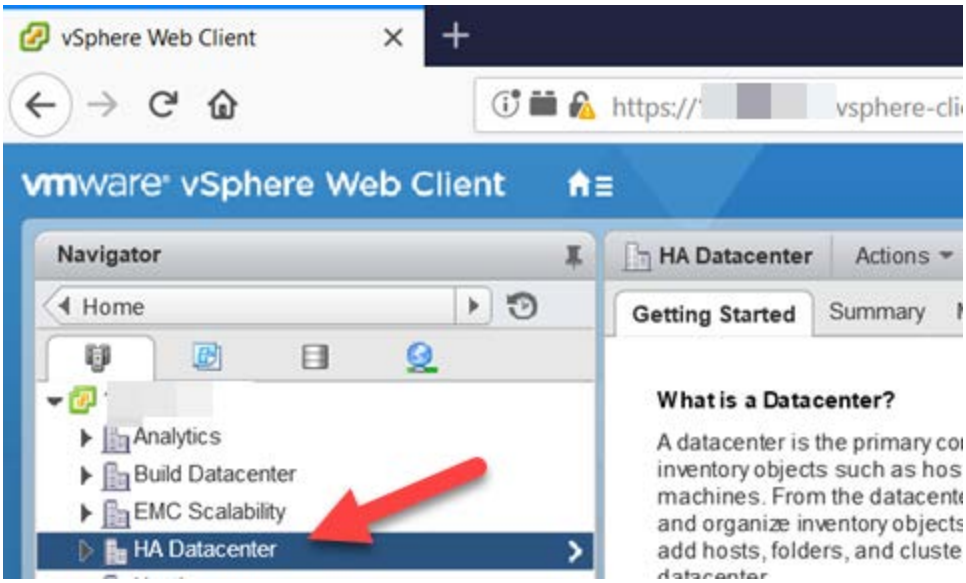
Enabling vSphere HA

When the licensed hosts are included in a cluster, you can enable vSphere HA using the cluster's settings in the New Cluster window. Refer to your VMware documentation for more information on configuring clusters.

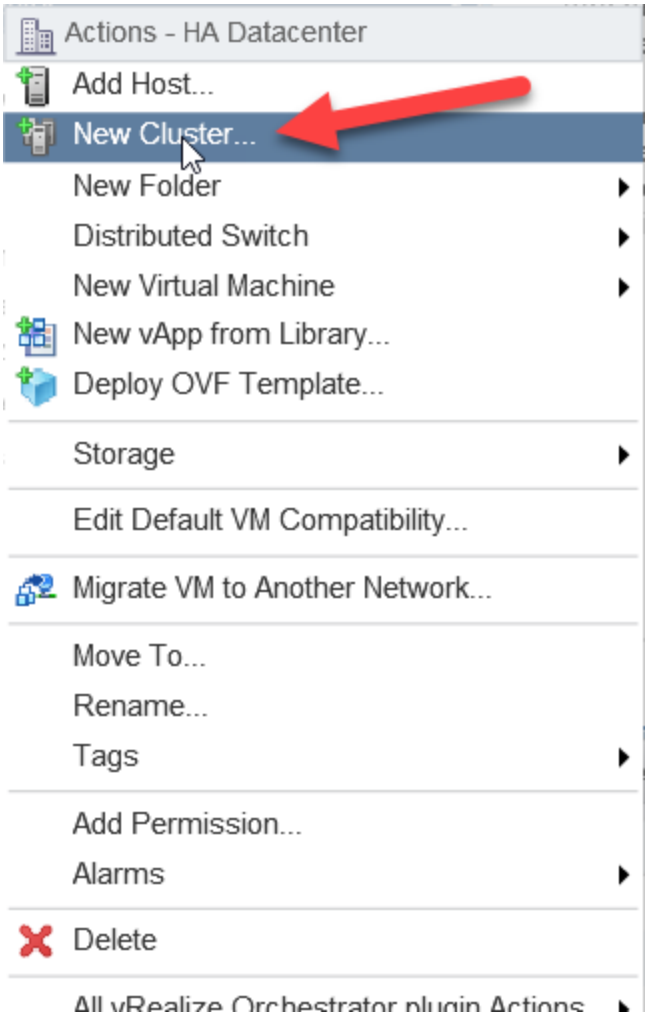
1. Log in to your vSphere Client.
2. Select **Hosts and Clusters** in the Inventories section.



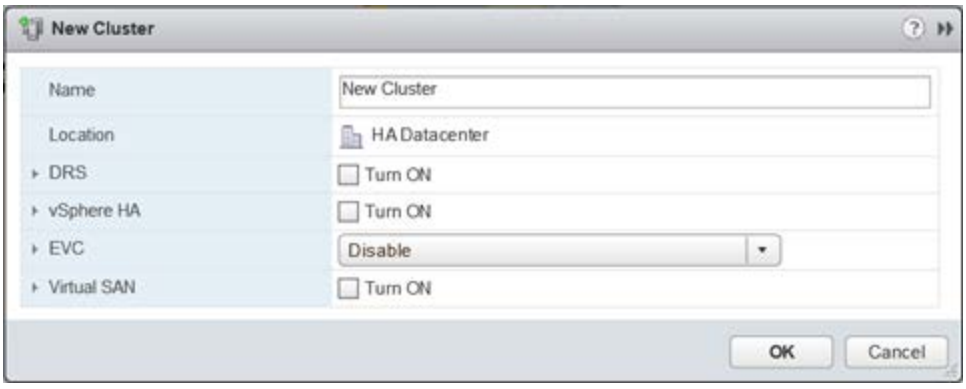
3. Select the datacenter in the left-panel on which you are adding the cluster.



4. Right-click the data center and select **New Cluster**.

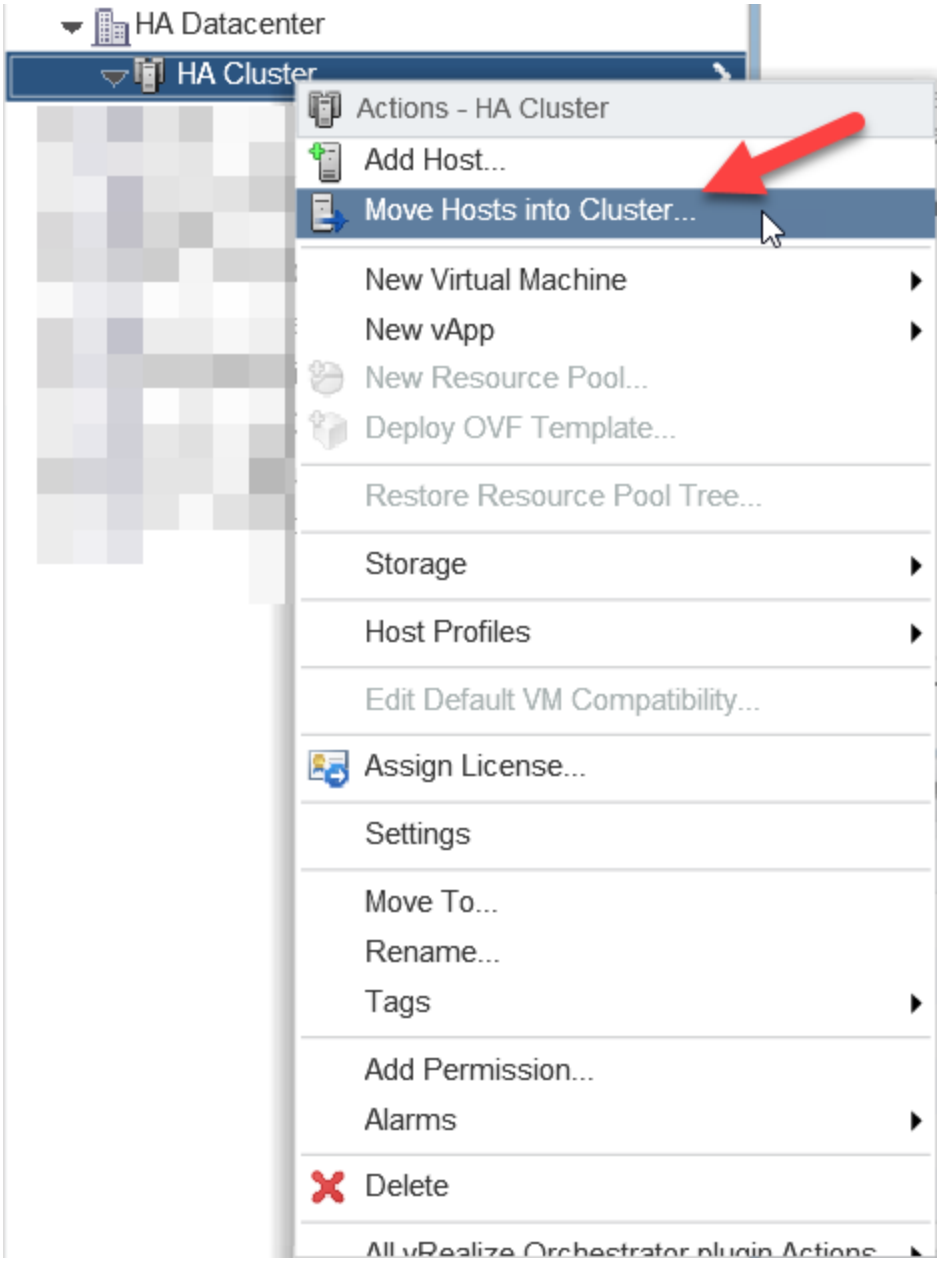


The **New Cluster** window displays.

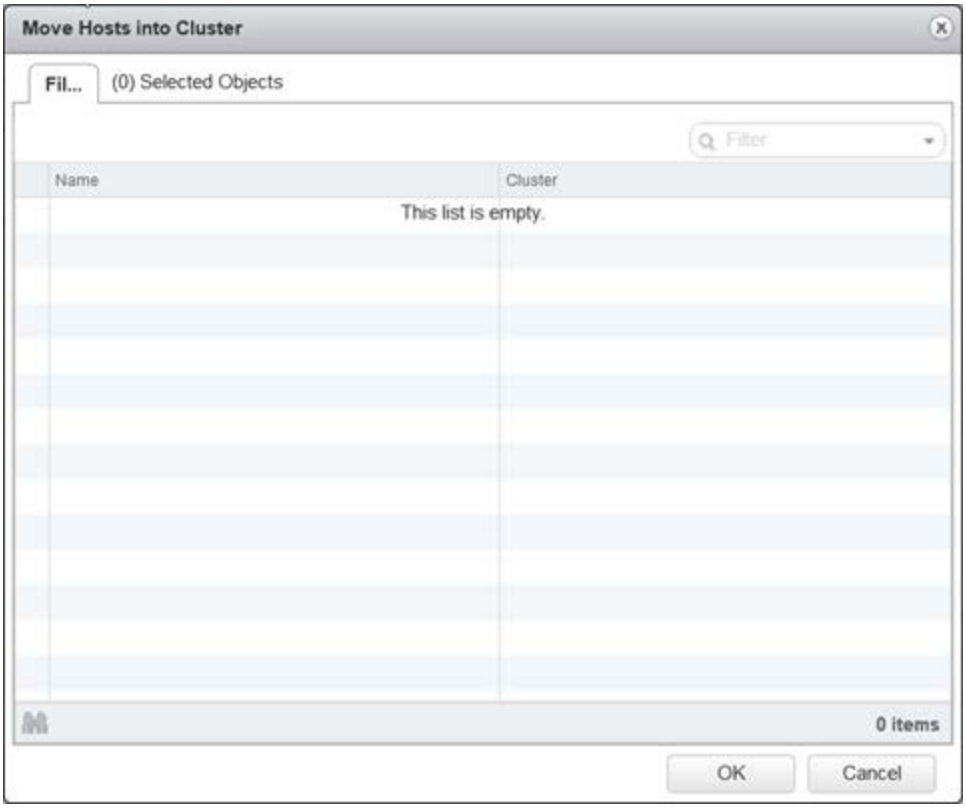


5. Configure the fields in the **New Cluster** window.
6. Select **vSphere HA** in the left-panel and select the box to enable.

7. Select **OK** to create an empty cluster.
8. Expand the datacenter in the left-panel so the cluster displays.
9. Right-click the cluster and select **Move Hosts into Cluster**.

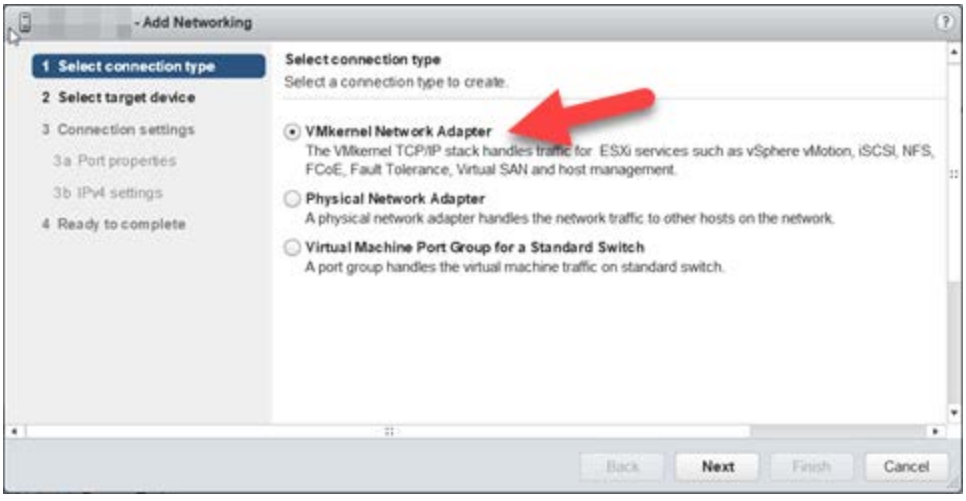


The **Move Hosts into Cluster** window displays.



10. Select the appropriate hosts to add to the cluster and select **OK**.
11. Expand the cluster in the left-panel.
12. Right-click a host from the left-panel and select **Add Networking**.

    The Add Networking wizard displays.



13. Select **VMkernal Network Adapter** and select **Next**.

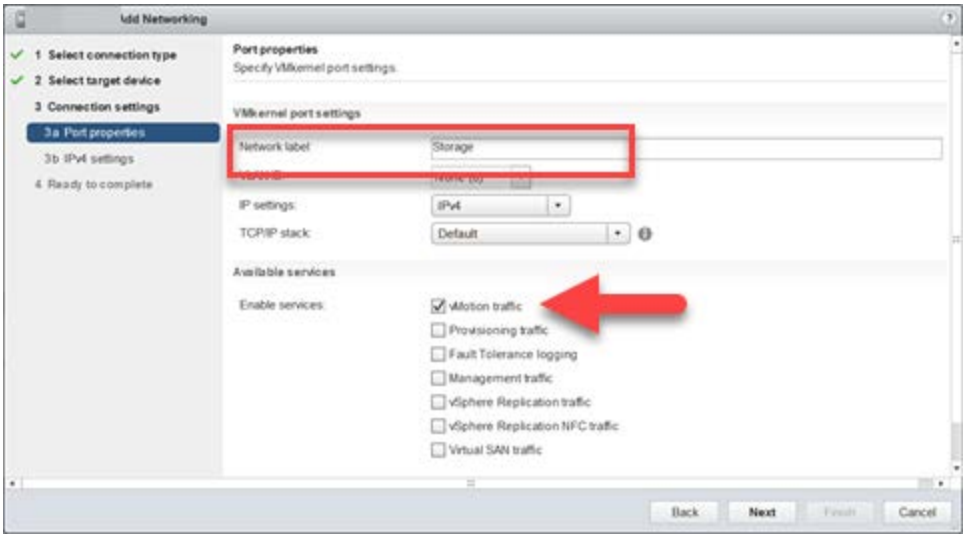
14. Select **Select an existing standard switch** radio button and select **Browse**.

    The **Select Switch** window displays.

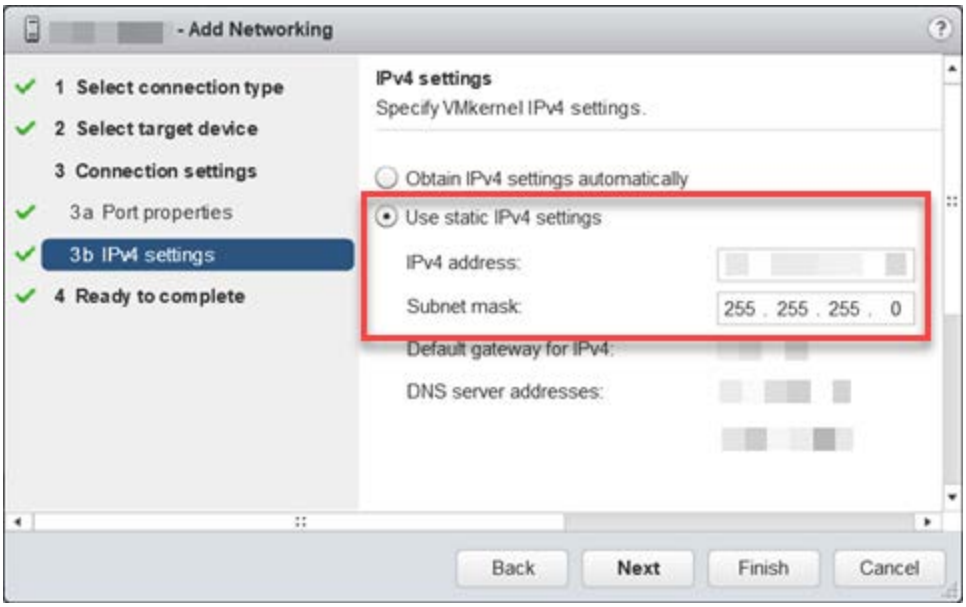
15. Select an unused existing vmnic from the list, select **OK**, and select **Next**.



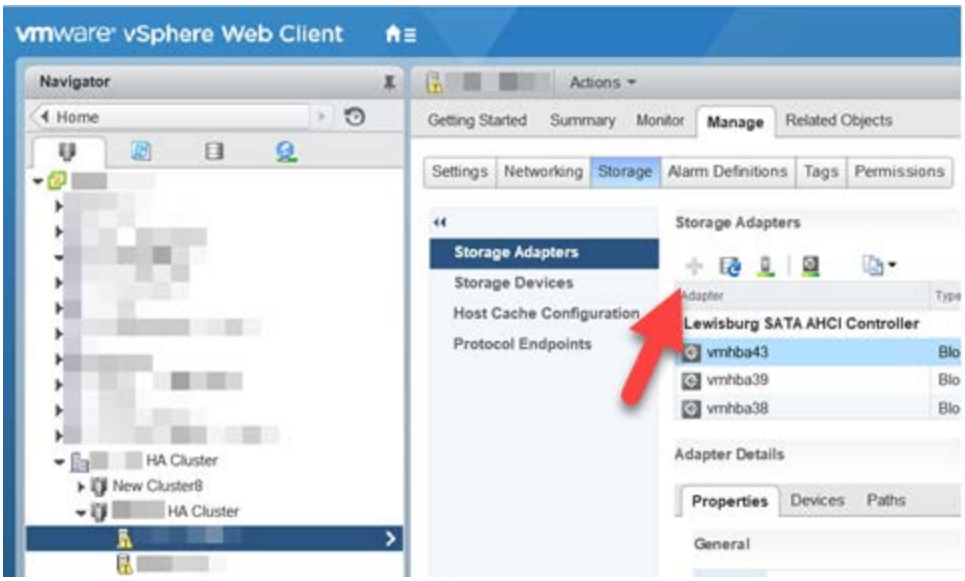
16. Enter **Storage** for Network label and select the **vMotion traffic** checkbox, then select **Next**.



17. Select **Use static IPv4** settings, enter the IP address for the storage server for the host being configured in the **IPv4 address** field, enter **255.255.255.0** in the **Subnet mask** field and select **Finish**.



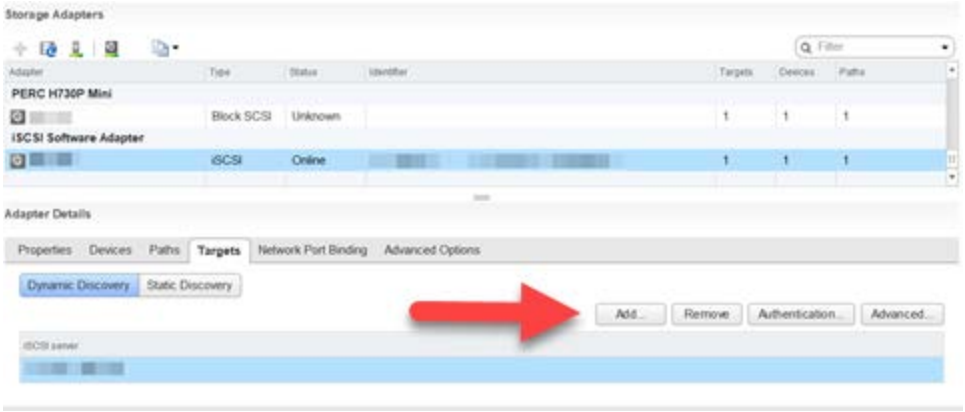
18. Repeat for all hosts in the cluster.
19. Select a host in the cluster in the left-panel and select the **Manage** tab.
20. Select **Storage**, **Storage Adapters**, and select the **Add** icon.



The adapter appears in the iSCSI Software Adapter section of the table.

21. Select the new adapter.
22. Select the **Targets** tab.

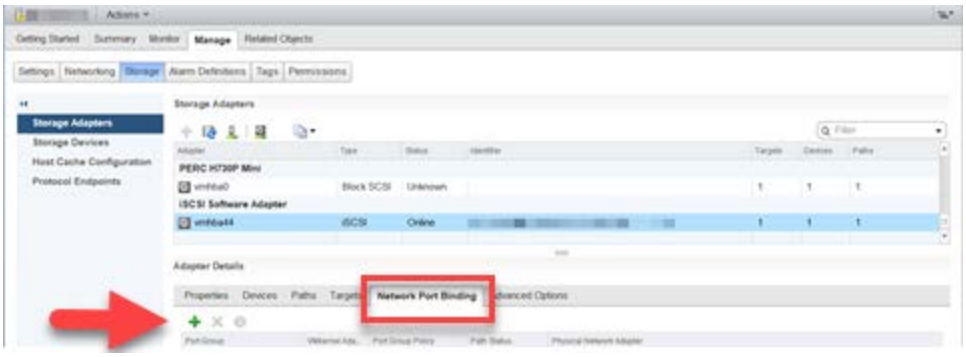
23. Select **Dynamic Discovery** and select **Add**.



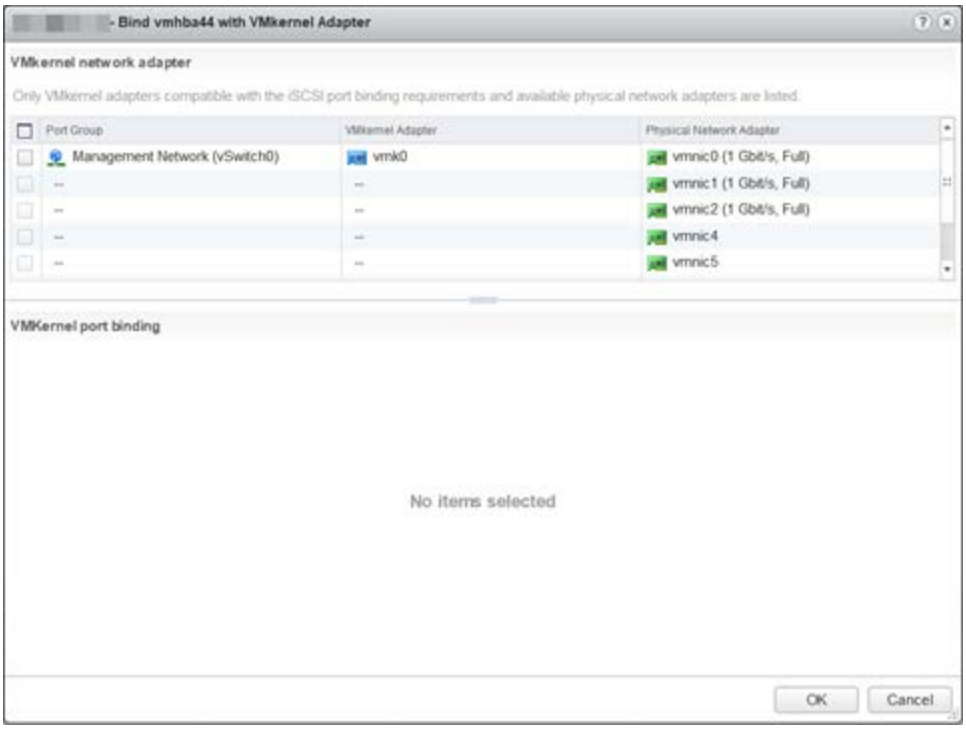
The **Add Send Target Server** window displays.



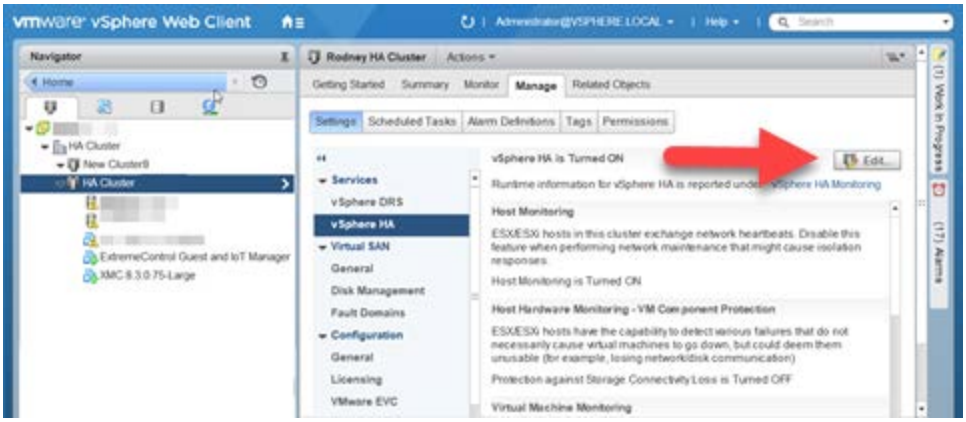
24. Enter the IP address of the storage server or full domain name in the **iSCSI Server** field and the port in the **Port** field.
25. Select **OK**.
26. Select the **Network Port Binding** tab and select the **Add** icon.



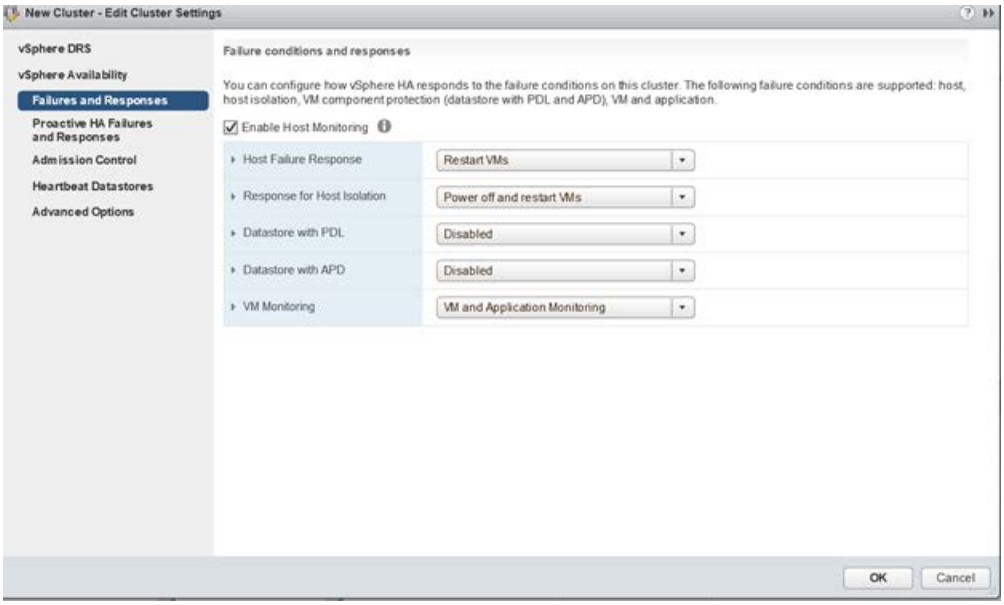
The **Bind with VMkernal Adapter** window displays.



27. Select the Storage created in Step 16.
28. Select the cluster you created in Step 6 in the left-panel.
29. Select the **Manage** tab in the right-panel and select **Settings**.
30. Select **vSphere HA** in the Services menu and select **Edit**.



The **Edit Cluster Settings** window displays.



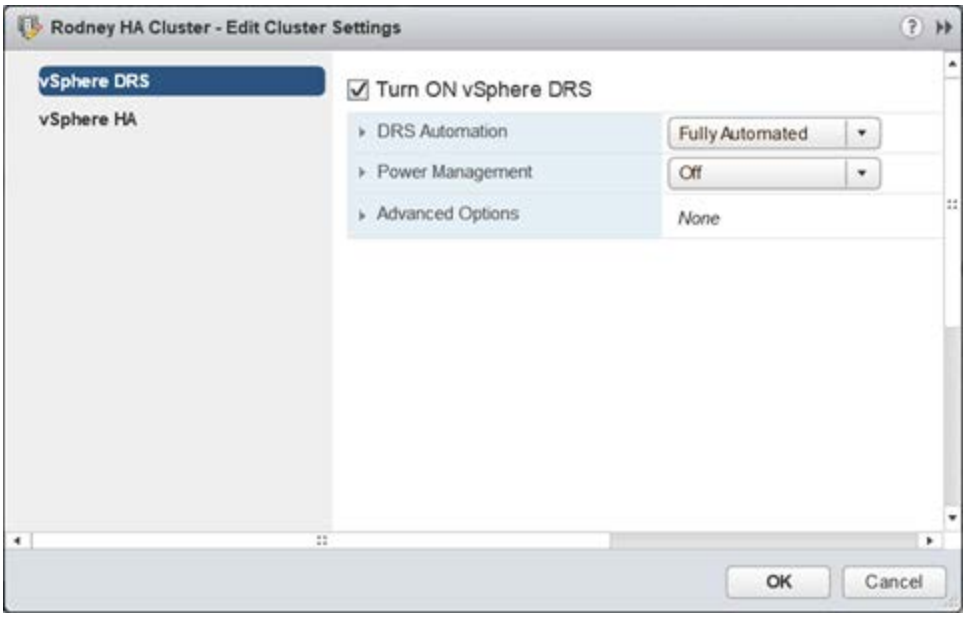
31. Select **Failures and Responses** in the left-panel.
32. Select the **Enable Host Monitoring** checkbox.
33. In the **Host Failure Response** drop-down list, select the action vSphere HA initiates if a host fails.
34. In the **Response for Host Isolation** drop-down list, select the action vSphere HA initiates if a host becomes isolated from the management network.

NOTE: Selecting **Leave Powered on** may cause impaired performance in ExtremeCloud IQ Site Engine or cause ExtremeCloud IQ Site Engine to become unresponsive.

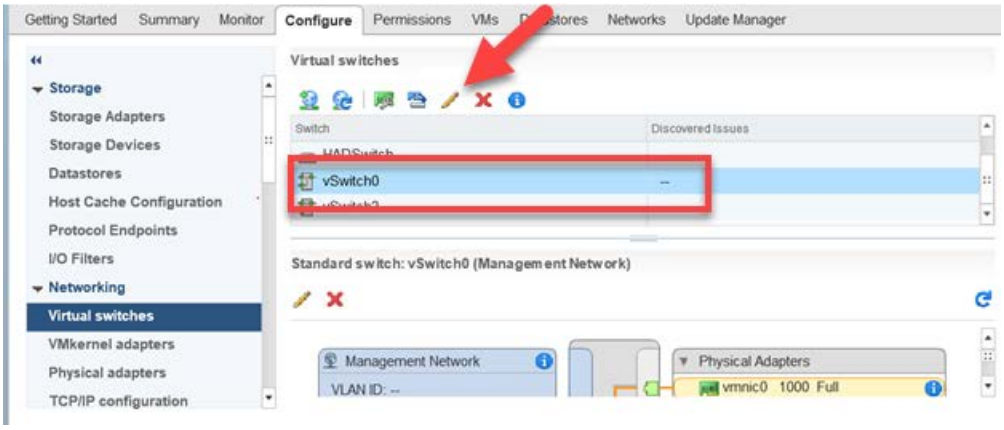
---

35. In the **VM Monitoring** drop-down list, select **VM Monitoring Only** or **VM and Application Monitoring**:
    - **VM Monitoring Only** — Virtual machines restart if vSphere does not receive the heartbeat within a certain amount of time.
    - **VM and Application Monitoring** — Enables ExtremeCloud IQ Site Engine monitoring via the Watchdog Service.
36. This is optional. In the **Datastore with PDL** and **Datastore with APD** drop-down lists, select a datastore to monitor hosts and virtual machines when the management network fails.

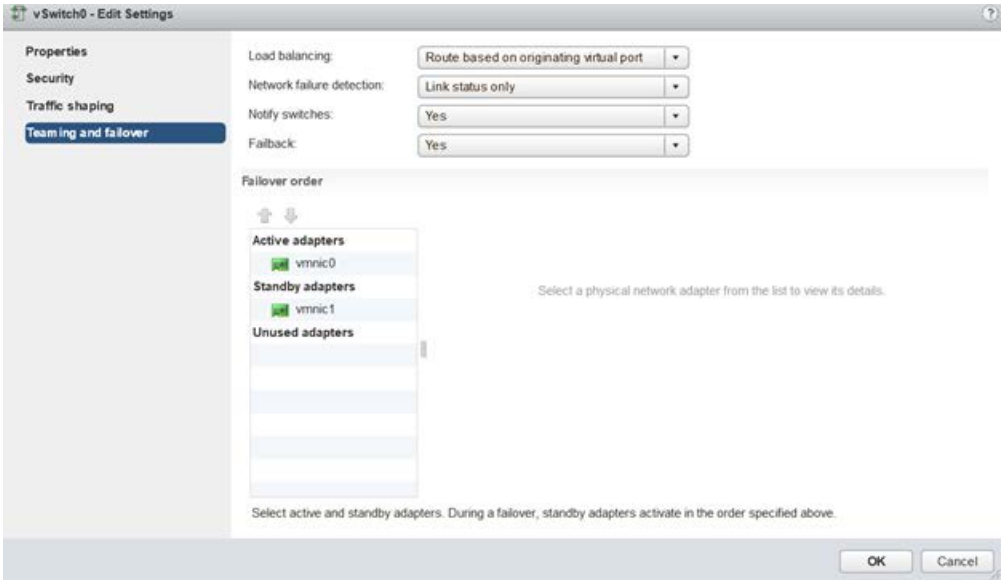
37. Select **vSphere DRS** in the left-panel of the window.



38. Select the **Turn ON vSphere DRS** checkbox.
39. Use the default values in the fields on this screen and select **OK**.
40. Additionally, you can create network redundancy on the host management network.
    a. Select the host, open the **Configure** tab, and select **Virtual switches** in the left-panel.
    b. In the Switch table in the right-panel, select the vSwitch on which you are configuring teaming and select the **Edit** icon.



The **Edit Settings** window displays.



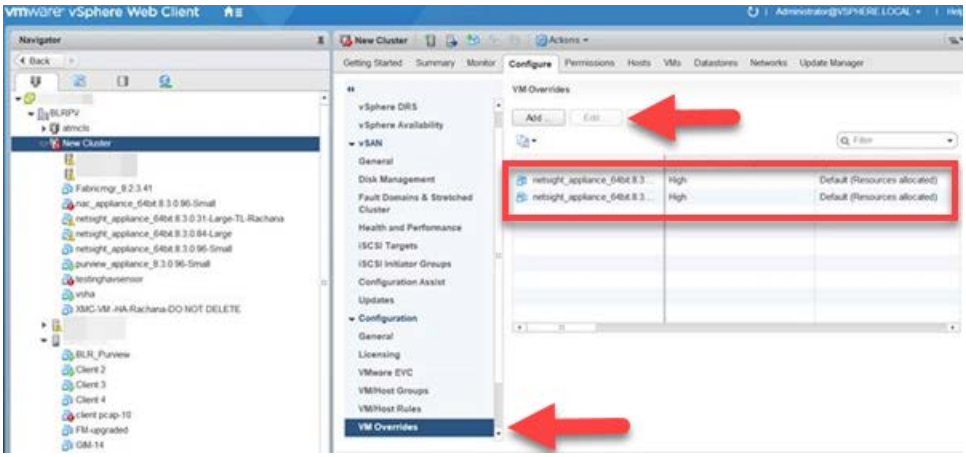
c. Select the appropriate teaming settings for the vSwitch.

d. Select **OK** to save.

ExtremeCloud IQ Site Engine Upgrade Process

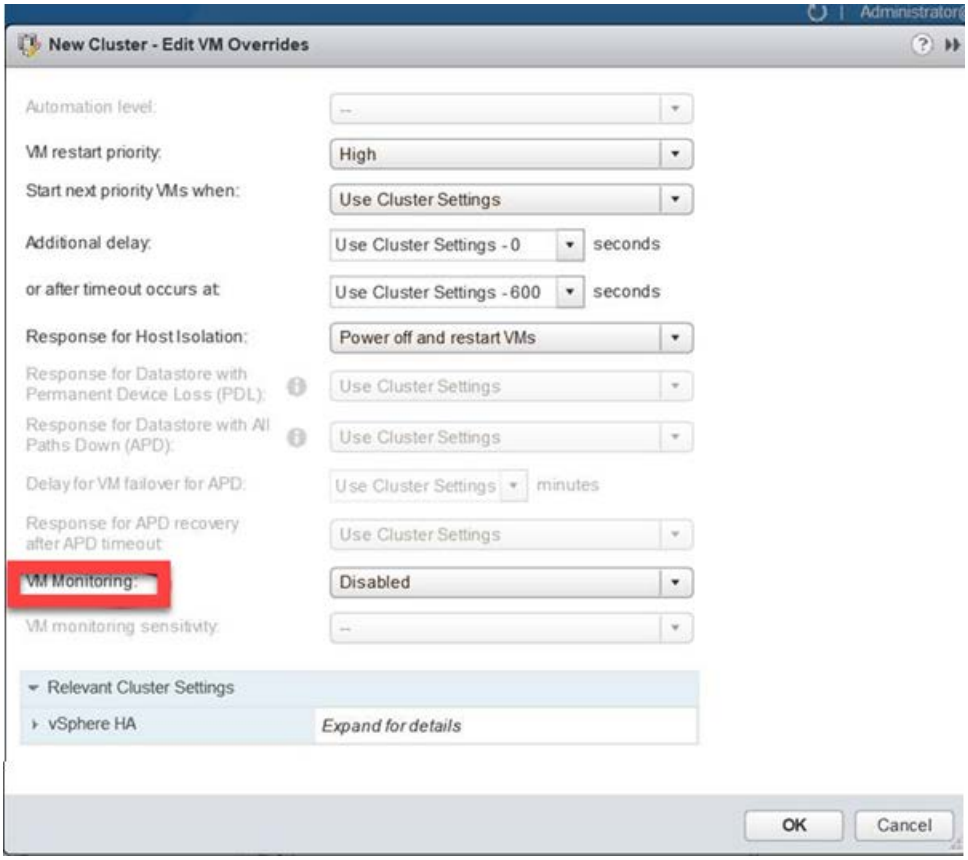
To upgrade an ExtremeCloud IQ Site Engine server on which VMware HA is currently configured, use the following instructions:

1. Log into your vSphere Client.
2. Select **Hosts and Clusters**.
3. Select the cluster on which HA is enabled.
4. Select the **Configure** tab in the right-panel and select **VM Overrides**.



5. Select the virtual machine for ExtremeCloud IQ Site Engine in the table and select **Edit**.

   The **Edit VM Overrides** window displays.



6. Select **Disabled** in the **VM Monitoring** drop-down list.
7. Select **OK**.
8. Upgrade ExtremeCloud IQ Site Engine.

9. Log into your vSphere Client.
10. Select **Hosts and Clusters**.
11. Select the cluster on which HA is enabled.
12. Select the **Configure** tab in the right-panel and select **VM Overrides**.
13. Select the virtual machine for ExtremeCloud IQ Site Engine in the table and select **Edit**.

    The **Edit VM Overrides** window displays.
14. Select **Enabled** in the **VM Monitoring** drop-down list.
15. Select **OK**.

High Availability Support for ExtremeCloud IQ Site Engine with vSphere Version 6.5

High Availability Support for ExtremeCloud IQ Site Engine with Hyper-V 2025