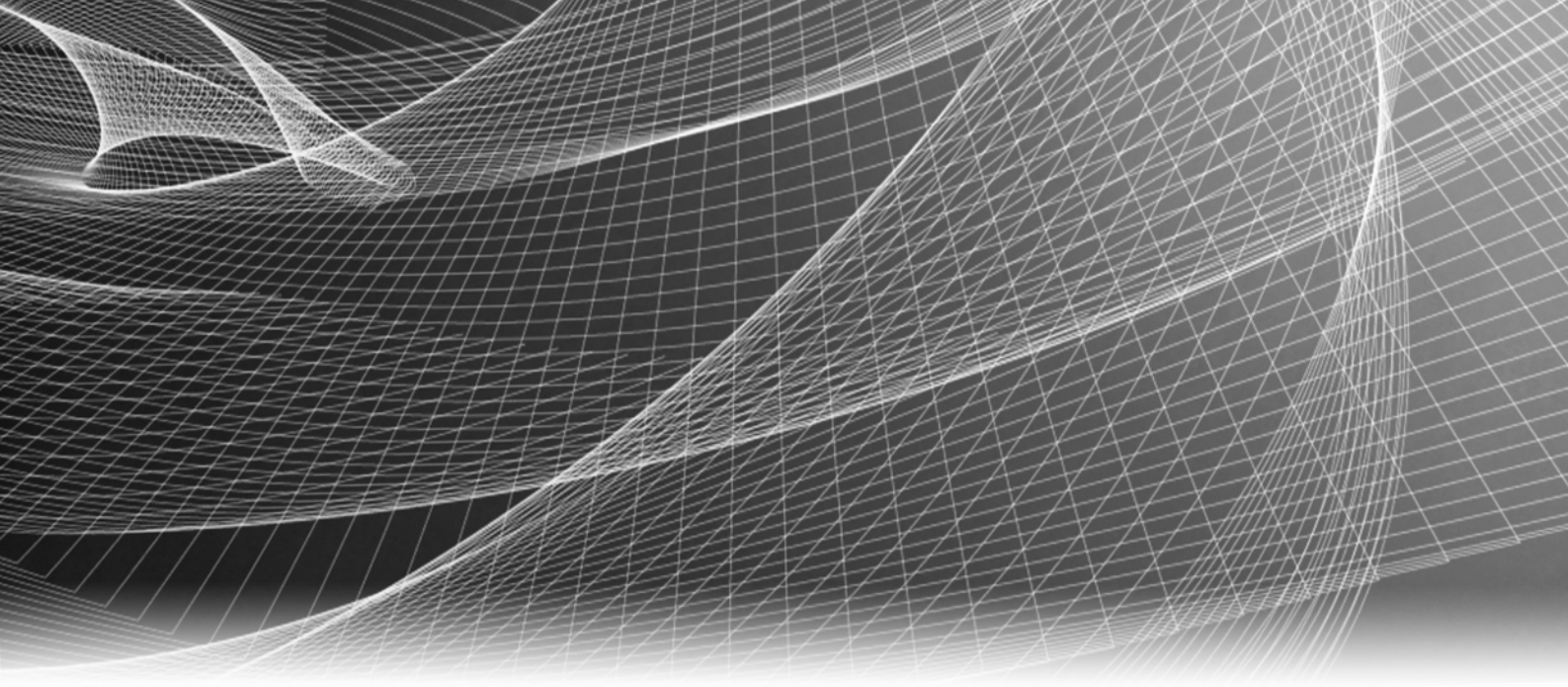


EMC® Secure Remote Services

Release 3.26

Site Planning Guide

REV 01

EMC²

Published January 2018

For the most up-to-date regulatory document for your product line, go to Dell EMC Online Support (https://support.emc.com).

CONTENTS

Preface

Chapter 1 Overview

ESRS architecture 10
ESRS installation options 10
Other components 11
Requirements for ESRS customers 11
Supported devices 12
Responsibilities for ESRS tasks 14
Customer 14
Customers and EMC Global Services 14
Site planning process 14
Coordination with EMC 15

Chapter 2 Component Requirements

Basics 18
Server types 18
Server requirements 18
Network requirements 18
Enabling communication to EMC 19
Enabling proxy server for ESRS traffic to EMC 19
Communication between Policy Manager and ESRSv3(s) 20
Communication between the ESRSv3(s) and devices 20
ESRSv3 with EMC managed products 21

Chapter 3 Configurations

Introduction 24
ESRS Version 3 24
Policy Manager 24
Device limits 24
Recommended ESRS configurations 26
High Availability ESRSv3 Cluster and Policy Manager 26
Single ESRSv3 and Policy Manager 27
Other supported configurations 28
High Availability ESRSv3 servers without Policy Manager 28
Single ESRSv3 server without Policy Manager 29
Topology and network considerations 30
Determining the quantity of ESRSv3 and Policy Managers 30
Installing a separate Policy Manager server 30
Protecting the ESRS server 30
Using proxy servers 31
Topology configurations 31
About the Policy Manager 35
Policy Manager authorization settings 35
Policy Manager failure 35
About not using a Policy Manager 35
High Availability ESRSv3 Clusters 36

High Availability ESRSv3 Cluster servers do not have failover 36
Failover behavior at the EMC device level 37
ESRSv3 configurations 37

Chapter 4 Preparing for Site Installation

Overview 40
Coordination with EMC 40
Preparation work 40
EMC coordination schedule 41
Kickoff meeting 41
Configuration planning and documentation meeting 43
Installation planning and scheduling meeting 45

Appendix A ERS Version 3 connections to/from EMC products

ESRSv3 GUI deployment suffixes. 48

Glossary

Index

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. Go to Dell EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This guide is part of the EMC Secure Remote Services (ESRS) Release 3.26 documentation set, and is intended for use by customers and prospective customers.

Readers of this guide are expected to be familiar with the following topics:

- Local network administration
- Internet protocols
- EMC storage system characteristics and administration

Related documentation

The following EMC publications provide additional information:

- *EMC Secure Remote Services Release Notes*
- *EMC Secure Remote Services Technical Description*
- *EMC Secure Remote Services Pre-Site Checklist*
- *EMC Secure Remote Services Site Planning Guide*
- *EMC Secure Remote Services Port Requirements*
- *EMC Secure Remote Services Installation Guide*
- *EMC Secure Remote Services Operations Guide*
- *EMC Secure Remote Services Policy Manager Operations Guide*
- *ESRS Policy Manager 6.8 Installation Guide - Standard Windows*
- *ESRS Policy Manager 6.8 Installation Guide - Integrated AD (Windows)*

Documentation conventions

EMC uses the following conventions for special notices:

DANGER

DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING

WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

CAUTION, used with the safety alert symbol, indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to personal injury.

Note: A note presents information that is important, but not hazard-related.

Typographical conventions

EMC uses the following type style conventions in this document:

Bold	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Use for full titles of publications referenced in text and for variables in body text.
`Monospace`	Use for: • System output, such as an error message or script • System code • Pathnames, file names, prompts, and syntax • Commands and options
`Monospace italic`	Use for variables.
`Monospace bold`	Use for user input.
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information — For documentation, release notes, software updates, or information about EMC products, go to Dell EMC Online Support at:

https://support.emc.com

Technical support — Go to Dell EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

techpubcomments@emc.com

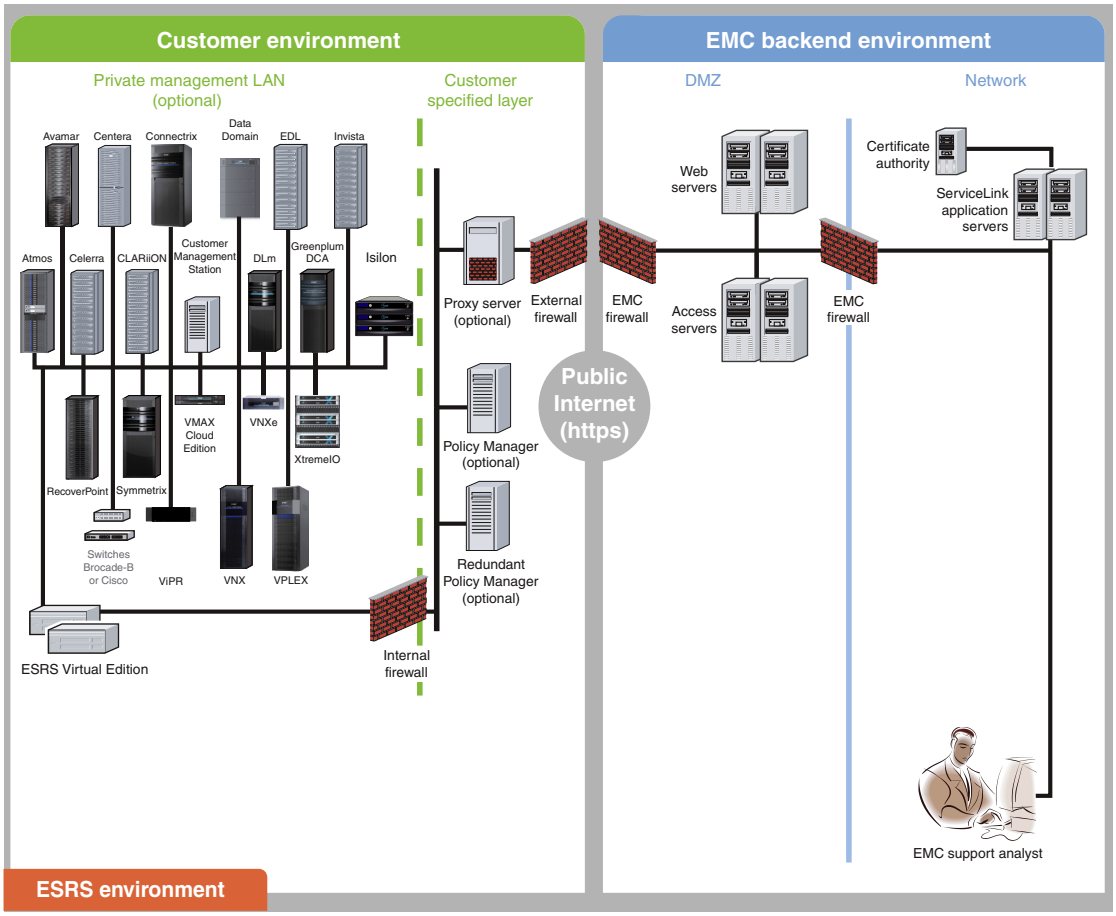
CHAPTER 1
Overview

This chapter provides an overview of EMC Secure Remote Services (ESRS) Release 3.26 architecture, lists supported devices, and describes the responsibilities for ESRS tasks. It also describes the process of working with EMC Global Services to prepare your site for your ESRS implementation. Topics includes:

- ESRS architecture 10
- Supported devices 12
- Responsibilities for ESRS tasks 14
- Site planning process 14
- ESRS architecture 10

ESRS architecture

EMC® Secure Remote Services Version 3 (ESRSv3) is an IP-based automated connect home and remote support solution enhanced by a comprehensive security system. ESRS creates both a unified architecture and a common point of access for remote support activities performed on your EMC products. For an illustration of the EMC Secure Remote Services architecture, see Figure 2 on page 10.



GEN-002137

Figure 2 **EMC Secure Remote Services (ESRS) architecture**

Note: Redundant Policy Manager is only supported on Policy Manager 2.02.1-xxx.

ESRS installation options

ESRSv3 includes the following options for installation at your site:

- **ESRS Virtual Edition (ESRS VE) —** This ESRS software can be installed on a customer-supplied VMware ESX or Microsoft Hyper-V Server. It can also be installed on multiple servers. The servers act as the single point of entry and exit for all IP-based remote support activities and most EMC connect home notifications.
- **ESRS Docker Edition (ESRS DE) installable on Linux host —** ESRS can be installed on a Linux host using the Docker Engine. Before installing ESRS on a Linux host, the following must already be installed:

  - Docker supported Linux distribution (x64 bit)
  - Docker Engine (Docker runtime)

  Using the binary installer, ESRS can be installed on the Linux distributions that support Docker. For a list of Linux distributions that are supported by Docker and for Docker installation instructions, refer to the following address:

  https://docs.docker.com/engine/installation

  For ESRS installation instructions on a Linux host, refer to the *EMC Secure Remote Services Installation Guide*.

  Note: Cloud platform support for the ESRS Docker Edition is best effort.

- **Policy Manager —** This software component is installed on a customer-supplied server or servers. It can be configured for the following:
  - Control remote access to your devices
  - Maintain an audit log of remote connection
  - File transfers Connect Homes by ESRS
  - Access to administration actions performed on the Policy Manager

Other components

EMC Secure Remote Services builds upon previous releases by providing many new features for remote notification and support.

Redundant Policy Manager option

ESRS provides the option to install a redundant Policy Manager. If the primary Policy Manager becomes unavailable, the redundant Policy Manager is used to resume operations. Both Policy Managers enforce the same policies. Manual failover is required. The failover is done via Policy Manager configuration in the ESRS GUI.

Note: Redundant Policy Manager is only supported on Policy Manager 2.02.1-xxx.

Security enhancements

ESRSv3 provides the enhanced security practices and encryption technologies, including:

- Certificate protected by RSA Lockbox Technology
- Advanced Encryption Standard (AES), SHA-2, 256-bit encryption between the ESRS and EMC
- Bilateral certificate authentication for all communication between the ESRSv3 and EMC
- Configurable security between ESRS components

Requirements for ESRS customers

ESRS customers must provide the following:

- VMware ESX Server 5.x or later
- Windows Hyper-V environment
- Linux host using the Docker Engine
- An IP network with Internet connectivity
- Capability to add ESRSv3 servers and Policy Manager servers to your network

- Network connectivity between the ESRSv3 servers and EMC devices to be managed by ESRS
- Internet connectivity to EMC's ESRS infrastructure by using outbound ports 443 and 8443

IMPORTANT

Port 8443 is not required for functionality, however without this port being opened, there will be a significant decrease in remote support performance, which will directly impact time to resolve issues on the end devices.

- Network connectivity between ESRSv3(s) and Policy Manager
- Mail server required for installation/optional FTPS

For additional requirements, see "Responsibilities for ESRS tasks" on page 14.

Supported devices

Table 1 on page 12 lists the EMC storage device models and environments supported by ESRS.

Table 1 **Product and application releases supported by ESRS(s)**

Product	Environment/application releases
EMC Atmos®	Atmos 1.4 or later
EMC Avamar®	Avamar 6.0 or later
EMC Caspian/Neutrino®	Contact your EMC representative
EMC Celerra®	NAS Code 5.4 or later
EMC Centera®	CentraStar® 2.4 or later [b]
EMC CLARiiON® CX, CX3, CX4, and AX4-5 Series storage systems *(distributed or Enterprise environments)*	FLARE® Operating Environment 2.19 or later Navisphere® Manager 6.19 or later **Note:** The AX-100/AX-150 are not supported as they do not support the required CLARalert.The AX4-5 series are supported only if the Navisphere Full license (with CLARalert) is purchased and installed on the storage system.
EMC CloudArray	Contact your EMC representative
CloudBoostAppliance	
EMC DPC CloudBoost	Contact your EMC representative
Customer Management Station	
Data Domain	DD OS version 4.8 or higher
Data Protection Advisor (DPA)	Contact your EMC representative
DellEMCSymphony	
EMC Disk Library for mainframe (DLm), Gen2	DLm 4020, DLm 4080, release 1.2 and later
EMC Disk Library for mainframe (DLm), Gen3	DLm 8000 3.4.0 & 3.4.1
	DLm 6000 All releases
	DLm 2000 All releases
	DLm 1000 3.5
EMC Disk Library for mainframe (DLm), Gen4	DLm 8100, DLm2100 with VNX, and DLm2100 with DD
EMC Disk Library (EDL)	DL-5100 and 5200 series DL-4000 series — DL-4100, DL-4106, DL-4200, DL-4206, DL-4400A/B, DL-4406A/B DL-700 series — DL-710, DL-720, DL-740 DL-310 DL3D 1500, 3000, 4000 — release 1.01 and later
EMC DSSD	Contact your EMC representative

Table 1 **Product and application releases supported by ESRS(s)**

Product	Environment/application releases
EMC Elastic Cloud Storage (ECS)	Contact your EMC representative
EMC Embedded NAS (eNAS)	Contact your EMC representative
EMC Enterprise Copy Data Management (eCDM)	Contact your EMC representative
EMC Greenplum® Data Computing Appliance (DCA)	Greenplum 4.0
EMC Invista®	Invista 2.2 or later
EMC Isilon®	OneFS 7.1
NetWorker	
EMC PowerPath®	Contact your EMC representative
EMC RecoverPoint	RecoverPoint 3.1, 3.2, 3.3, 3.4 and later [a]
EMC ScaleIO®	Contact your EMC representative
EMC Symmetrix® 8000 Series	Enginuity™ 5567 and 5568 with Service Processor Part Number [c] 090-000-064, 090-000-074, or 090-000-09*x*
Symmetrix DMX™ Series	Enginuity 5670, 5671
Symmetrix DMX-3 Series	Enginuity 5771, 5772, 5773
Symmetrix DMX-4 Series	Enginuity 5772, 5773
Symmetrix VMax™ Series	Enginuity 5874, 5875
Symmetrix Device Client	Enginuity 5670, 5671, 5771, 5772, 5773, 5874, 5875
EMC Unity/UnityVSA™	Contact your EMC representative
VCE Vision	Contact your EMC representative
EMC ViPR®	Contact your EMC representative
EMC ViPR SRM	Contact your EMC representative
EMC VMAX³	Enginuity 5977
EMC VNX®	VNX Operating Environment (OE) for Block 05.31.000.5.006 or greater VNX Operating Environment (OE) for File 7.0.12.0 or greater
VNX Control Station Device Client	VNX Operating Environment (OE) for Block 05.31.000.5.006 or greater VNX Operating Environment (OE) for File 7.1.44 or greater
EMC VNXe®	VNXe 2.0.x
VNXe Device Client	VNXe 2.0.x
EMC VPLEX®	GeoSynchrony 4.0.0.00.00.11 or later
EMC VxRail (VSPEX BLUE®)	Contact your EMC representative
EMC XtremIO®	XtremIO 2.2.x and greater
XtremIO Device Client	XtremIO 2.2.x and greater
Switch - Fabric Manager managing Brocade B-series switches	• Brocade B-series switches running Fabric OS 5.0.1b through 6.1.0x only, with Fabric Manager 5.2.0b or later [b d e g] • Brocade switches without monitoring (connect in support only, no connect home)
Switch - Cisco	• Cisco MDS switches running SAN-OS 3.1(2) or later, NX-OS 4.1(1b) or later. [b] • Nexus switches running NX-OS 4.2(1)N1(1) or later. [b h] **Note:** MDS switches require Fabric Manager or Cisco Data Center Network Manager (DCNM) to be the same version or higher than the highest switch firmware version. Nexus requires Fabric Manager 5.0(1a) or higher.

a. RecoverPoint 3.1 and 3.2 utilize ESRS for remote support access only. RecoverPoint 3.3 and later add the connect home feature. RecoverPoint Management GUI (RPMAGUI) is supported on Gateway Client code 2.20 and above
b. For remote support access only, not for connect home through ESRS IP.
c. These part numbers designate Service Processor that is running Windows NT SP6. xx70 code only supports ftp for connect home.
d. Fabric Manager does not support FOS 6.1.1 or higher. CM or CMDCE is required. Please refer to the appropriate FOS Release Notes.
e. CM does not support FOS 6.3.x or higher. cmdce is required. Please refer to the appropriate FOS Release Notes.
f. CMDCE is required to support FOS 6.3.x or higher. Please refer to the appropriate FOS Release Notes.
g. connect home via CM, CMDCE, or CMCNE, otherwise no connect home through ESRS Client.
h. connect home via Cisco Fabric Manager or Cisco Data Center Network Manager, otherwise no Connect Home through ESRS Client.

Responsibilities for ESRS tasks

This section defines who is responsible for various ESRS tasks including installation, configuration, operation, and maintenance.

Customer

The EMC customer is responsible for the following tasks:

- Providing ESX/Hyper-V Server(s)/Linux host using the Docker Engine
- Maintaining internet connectivity
- Preparing and configuring the network, Proxy Server, and firewall
- Preparing the servers for installation. This includes:
  - Preparing the ESRS VM, Hyper-V instance(s), or Linux Distribution
  - Preparing the Policy Manager server hardware and operating system
  - Placing the ESRSv3 and Policy Manager servers on the IP network
  - Maintaining Network Connectivity between ESRSv3 and EMC
  - Maintaining Network Connectivity between ESRSv3 and Managed Devices
  - Maintaining Network Connectivity between ESRSv3 and Policy Manager
  - Configuring, administering, and updating policy management activities, policies, and accounts on the Policy Manager
  - Backing up and restoring ESRS Virtual Appliance. Backing up, cloning, or making snaps of ESRSv3 could result in the MAC address changing, resulting in a loss of connectivity until the network interface is corrected.
  - Providing continuing maintenance, including security and operating system updates and upgrades on the ESRSv3 and Policy Manager servers
  - Providing physical security of all hardware
  - Protecting all files on the servers, including the Transport Layer Security (TLS) certificate, if applicable

Customers and EMC Global Services

Customers and EMC Global Services personnel are able to perform the following tasks:

- Installing the ESRSv3 software and Policy Manager software
- Configuring and deploying EMC product managed devices
- Configuring, testing, and verifying connect home
- Updating the ESRSv3 and Policy Manager software

Site planning process

EMC Secure Remote Services requires customer-provided components and actions. Your network, storage system, and security administration personnel must prepare your site for ESRS software installation.

This guide provides detailed instructions for completing each step in the customer site planning process. You should plan your solution deployment and schedule. Consult your EMC Global Services representative if you require assistance.

Coordination with EMC

This is a recommended schedule of preparation coordination meetings and activities with EMC and your internal network, storage, and security teams if you require assistance from EMC Global Services:

- Your teams should meet with EMC Sales and EMC Global Services to receive an ESRS review and get answers to your initial questions.
- You should host an onsite meeting for EMC Global Services and your teams to finalize and record your ESRS system configuration.
- Your teams should meet with EMC Global Services to finalize the solution deployment schedule and details.

For additional details about these meetings, see Chapter 4, "Preparing for Site Installation."

CHAPTER 2
Component Requirements

This chapter describes the requirements for the EMC Secure Remote Services (ESRS) server hardware and software that you must provide as part of the total configuration. Topics include:

- Basics 18
- Server requirements 18
- Network requirements 18

Basics

To properly support the ESRS configuration you choose, EMC recommends that you become familiar with the requirements of each software and hardware component. This chapter provides the requirements of each component.

IMPORTANT

Be sure to read Chapter 3, "Configurations" to define your configuration type and determine if you will need additional servers.

Server types

The customer must provide the following server types:

- ESX Server for creating Virtual Machine for configuring ESRS or Windows Hyper-V environment
- A separate ESX Server/Windows Hyper-V/Linux Distribution environment is needed for a high availability configuration (optional)

For detailed server requirements, refer to "Server requirements" on page 18.

Server requirements

ESX Server(s) must meet the hardware and operating system requirements listed in Table 2 on page 18.

Table 2 **ESRS server requirements**

Hardware	Software
ESX Server for creating Virtual Machine (VM) for configuring ESRS. An additional server could be used to setup an HA Cluster (optional). ESRS can be installed on: • VMWare ESX Server 5.x or later • Windows Hyper-V environment • Linux host using the Docker Engine. ESRS VM created on an ESX Server should support the following minimum configuration: **CPU** — One virtual CPU 2.2 GHz or higher, 64-bit **Memory** — 4 GB Memory or higher **Free Disk Space** — 64 GB minimum **Browser —** Microsoft Internet Explorer 9 or higher, or Google Chrome **Network** — Servers are attached to network **Comm —** Minimum single 10/100 Ethernet adapter (may require dual 10/100 Ethernet depending on customer network configuration and environment), preferred Gigabit Ethernet adapters, optional additional NIC for data backups **Note:** Contact EMC Global Services if your configuration does not meet the minimum hardware requirements. **Note:** ESRSv3 cannot be clustered with ESRS 2.x gateways or the ESRS device client.	ESX Server needs to support the minimum requirements for installation of ESRS software.

Network requirements

Before EMC Secure Remote Services goes online, you must ensure your network meets the following requirements:

- Network Address Translation (NAT) is supported between the ESRS Client and EMC Enterprise.
- Port Address Translation (PAT) cannot be used for the IP addresses of any EMC devices managed by the ESRSv3.
- Dynamic IP addresses (DHCP) should not be used for any components of the ESRSv3 servers, Policy Manager servers, or managed devices.

  Note: If you use DHCP to assign IP addresses to any ESRS components (ESRSv3 servers, Policy Manager, or managed devices), they must have "static" IP addresses. Leases for the IP addresses that EMC devices use cannot be set to expire. EMC recommends that you assign static IP addresses to those devices you plan to have managed by ESRS.

- Routes must exist from each of your managed devices to each of your ESRSv3 servers.
- The Policy Manager must be reachable by all ESRSv3 servers.

Enabling communication to EMC

All communication between the EMC devices at your site and EMC Global Services is initiated by, and occurs through, an ESRS Virtual Appliance at your site over the outbound default port 443 and 8443. Your firewall administrators must open port 443 and 8443 *outbound* to enable communication between the ESRS Virtual Appliance and EMC.

IMPORTANT

Port 8443 is not required for functionality, however without this port being opened, there will be a significant decrease in remote support performance, which will directly impact time to resolve issues on the end devices.

Enabling proxy server for ESRS traffic to EMC

ESRS supports the use of a proxy server for routing outbound Internet traffic from the ESRSv3(s) to EMC.

If you use a proxy server for outbound Internet traffic, you must make sure the proxy server:

- Can communicate with the ESRSv3(s) over an agreed-upon port.
- Can communicate with EMC, outbound, over TLS port 443 and 8443.

IMPORTANT

To ensure communication integrity, proxy servers and devices external to your DMZ must not perform any method of SSL decryption on outbound or inbound traffic for ESRS. SSL decryption performed on outbound communication by customer firewalls, proxies, Web traffic filtering appliances or cloud services, Web traffic shaping/load balancing, certificate verification, proxying, or Intrusion Detection Services (IDS) will cause a loss of connectivity to EMC.

Note: The customer is responsible for Proxy Server configuration. User account(s) should be service accounts that do not have expiring passwords.

The following proxy servers have been tested for use with ESRS.

Note: Configuration and operation are the Customer's responsibility.

- Linux Squid (supported in Red Hat 6.1 and 6.2)
- Apache HTTP Server release 1.1 and later (contains mod_proxy module)
- Microsoft ISA
- Netscape iPlanet Proxy Server release 3.6
- DeleGate 7_9_3

ESRS supports the following protocols for use with a proxy server:

- HTTP Proxy releases 1.0 and 1.1 (Username/Password is optional. If a username is provided s password is required)
- SOCKS releases 4 and 5 (may require username and password authentication)

Note: ESRS supports basic authentication for HTTP and SOCKS proxy servers, with or without credentials based on the proxy setup.

Communication between Policy Manager and ESRSv3(s)

The Policy Manager application *only* responds to communication requests from the ESRSv3(s).

At startup, the ESRSv3 registers Managed devices AND queries the Policy Manager for policies. The ESRSv3 then caches the permission rules. It then periodically polls the Policy Manager for configuration updates and audit logging.

The Policy Manager is an HTTP listener. You must configure the Policy Manager and ESRSv3 to use an agreed-upon port and protocol. EMC recommends that you use port 8443 for TLS-enabled HTTPS or port 8090 for standard HTTP. If necessary, you can specify a different port during the Policy Manager and ESRSv3 installations.

Note: If you are running Policy Manager in a Windows Server 2008 environment, you must configure the Windows firewall to permit traffic to the Policy Manager on both ports 8090 and 8443 (default). The firewall is closed by default and must be specifically configured to permit the Policy Manager traffic.

Communication between the ESRSv3(s) and devices

There are two connection requirements between the ESRSv3 and your managed devices:

- The first is the communication between the ESRSv3 and your managed devices connections. The ESRSv3 secures remote access connections to your EMC devices by using a session-based IP port-mapped solution.
- The second communication requirement is between your managed devices and the ESRSv3 for Connect Home messages. For those devices that use the ESRSv3 to forward Connect Home transfers, the transfer is sent through a secure encrypted data tunnel to EMC and an audit of the transfer is maintained on the Policy Manager.

ESRSv3 with EMC managed products

To enable communication between the ESRSv3 and your devices, you must configure your internal firewalls to allow traffic over the specific ports detailed in the *ESRS Port Requirements* document. These tables identify the installation site network firewall configuration open-port requirements for ESRS. The protocol/port number and direction are identified relative to ESRSv3 servers and storage devices. Figure 3 on page 21 provides a representation of the connections between devices, the ESRSv3, and EMC.

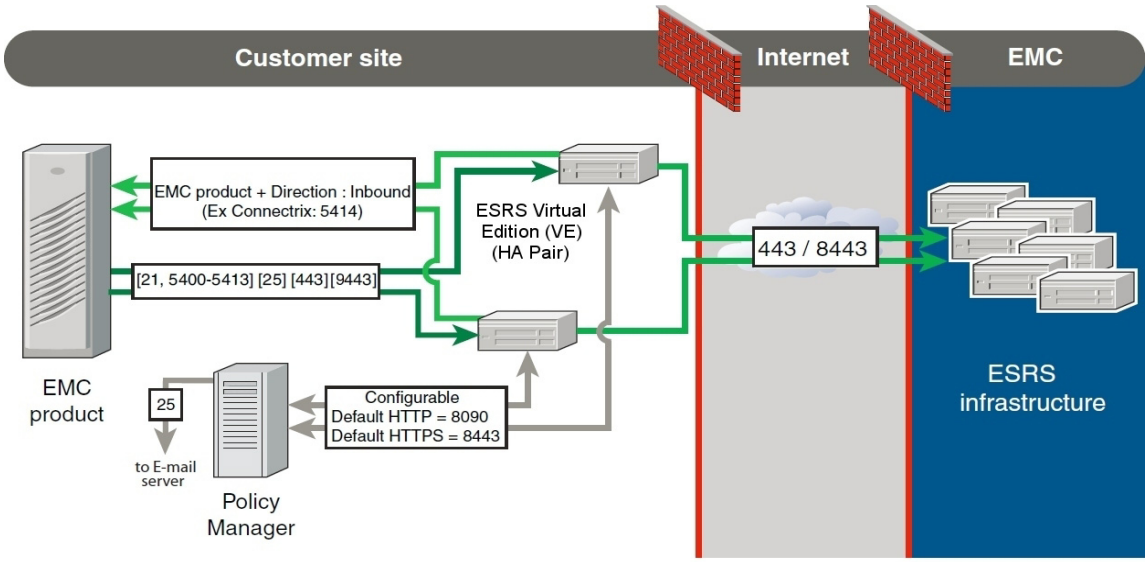


Figure 3 **Port diagram of ESRSv3 with EMC managed product**

Note: Refer to the *EMC Secure Remote Services Port Requirements* document for detailed port information.

CHAPTER 3
Configurations

This chapter describes the EMC Secure Remote Services (ESRS) configurations supported by EMC and provides recommendations for choosing a configuration and topology for your site. Topics include:

- Introduction 24
- Recommended ESRS configurations 26
- Other supported configurations 28
- Topology and network considerations 30
- About the Policy Manager 35
- High Availability ESRSv3 Clusters 36

Introduction

EMC recommends specific EMC Secure Remote Services component configurations. Both types of configurations are discussed in this chapter. EMC supports, but does not recommend, certain other configurations.

Note: In addition to the specifications described in the following sections, there are limits on the quantity of devices that can be safely managed on each server. There is a limit of 250 devices per ESRSv3 server/ESRSv3 Cluster (each deployed VNX or Unity Storage Processor counts as a separate device) and 750 devices per Policy Manager. "Device limits" on page 24 provides detailed examples of device and server limits.

There are two main ESRS software components that reside at a site:

- ESRSv3
- Policy Manager

ESRS Version 3

The ESRS Version 3 (ESRSv3) is the application installed on an ESX Server, Hyper-V Server, or Linux Distribution with the following requirements:

- ESX/Hyper-V server for deploying the ESRS VE template
- Linux host running the Docker Engine for deploying ESRS DE template
- For a High Availability configuration, two of these servers are required (optional)

Policy Manager

The Policy Manager may also be configured on multiple servers for redundancy.

Note: ESRS is supported for use with any version of Policy Manager (2.02.1-xxx, 6.6 ,or 6.8).

Note: Colocation of the Policy Manager on the ESRS Virtual Appliance is NOT supported.

Device limits

The ESRSv3 and Policy Manager components have the following device limits to help ensure reliable performance:

ESRSv3 — The recommended device limit for each ESRS Virtual Appliance or cluster is 250 devices. The device limit was developed by using remote session performance data and historical statistics about the number of remote sessions and devices in the field. By limiting the number of devices that can be deployed on an ESRS Virtual Appliance, remote servicing of equipment can be continued during periods when there might be numerous remote connections due to several concurrent problems.

Note: There is currently no software block that will stop the deployment of more than 250 devices. However, exceeding this recommended limit may cause an unacceptable level of throughput for remote connections during periods of peak usage. This can result in poor remote application performance, the inability to service some devices and/or being unable to process and forward device connect homes in a timely manner. The performance and behavior of the Policy Manager may also be significantly impacted.

Policy Manager — The recommended device limit for each Policy Manager is 750 devices. This limit enables the Policy Manager to retain spare bandwidth that may be needed during times of high activity.

⚠CAUTION

Exceeding the maximum device limits may cause performance degradation, resulting in remote access support limitations and a loss of connect home capabilities. Policy Manager Database failure / corruption could result in the loss of auditing of remote session approvals, connect home file uploads, configuration changes, and Policy Manager access audits. Policy Manager database corruption may also have significant impact on EMC's ability to provide remote support.

Table 3 **ESRS configuration examples for maximum devices**

	Configuration	Maximum devices	Policy Manager	Total servers
Site 1	Clustered HA servers group 1	250	Server No. 1 (servicing 6 ESRSv3, 750 devices)	7
	Clustered HA servers group 2	250		
	Clustered HA servers group 3	250		
	Clustered HA servers group 4	250	Server No. 2 (servicing 6 ESRSv3, 750 devices)	7
	Clustered HA servers group 5	250		
	Clustered HA servers group 6	250		
	Total maximum devices	1500		14
Site 2	Single ESRSv3 server 1	250	Server No. 1 (servicing 3 ESRSv3, 750 devices)	4
	Single ESRSv3 server 2	250		
	Single ESRSv3 server 3	250		
	Single ESRSv3 server 4	250	Server No. 2 (servicing 3 ESRSv3, 750 devices)	4
	Single ESRSv3 server 5	250		
	Single ESRSv3 server 6	250		
	Total maximum devices	1500		8

Recommended ESRS configurations

EMC has the following recommended configurations for ESRS:

- High Availability ESRSv3 Cluster and Policy Manager (preferred configuration)
- Single ESRSv3 Server and Policy Manager

The following section describes these recommended configurations.

High Availability ESRSv3 Cluster and Policy Manager

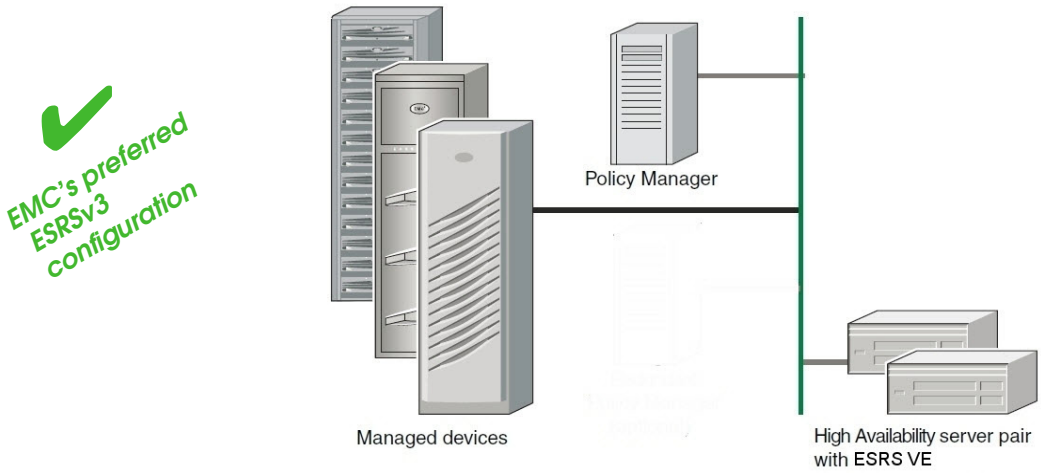


Figure 4 **Clustered HA ESRSv3 servers and Policy Manager**

EMC's preferred configuration for ESRS is the **High Availability ESRSv3 Cluster and Policy Manager** configuration shown in Figure 4 on page 26.

Once the cluster relationship is established, devices may be deployed on any of the clustered ESRS servers and are managed by *all* ESRS servers in the High Availability solution. Each server serves as a peer for the other servers in the cluster relationship. Each server monitors all devices, and any of the clustered servers can provide remote support access and/or connect home activity. Although they are peers monitoring the same devices, servers do not talk to each other.

The Policy Manager provides auditing of connect homes and script execution on the ESRS. The Policy Manager also provides auditing and access control to managed devices.

If you implement the High Availability ESRSv3 Cluster and Policy Manager configuration, the Policy Manager will not be impacted by failure of the ESRS Virtual Appliance.

The **High Availability ESRSv3 Cluster and Policy Manager** configuration has the following characteristics:

- **Number of required servers:** 3 (minimum)
- **Pros**:
  - The Policy Manager provides auditing and access control for the solution.
  - The cluster configuration provides connect home and remote support connection redundancy.
  - In the event of a server hardware failure, the cluster configuration allows for easy recovery of the failed ESRSv3.

- **Con**: Multiple servers are required.

Note: ESRSv3 cannot be clustered with ESRS 2.x gateways or the ESRS device client.

Single ESRSv3 and Policy Manager

Easily upgraded to preferred configuration

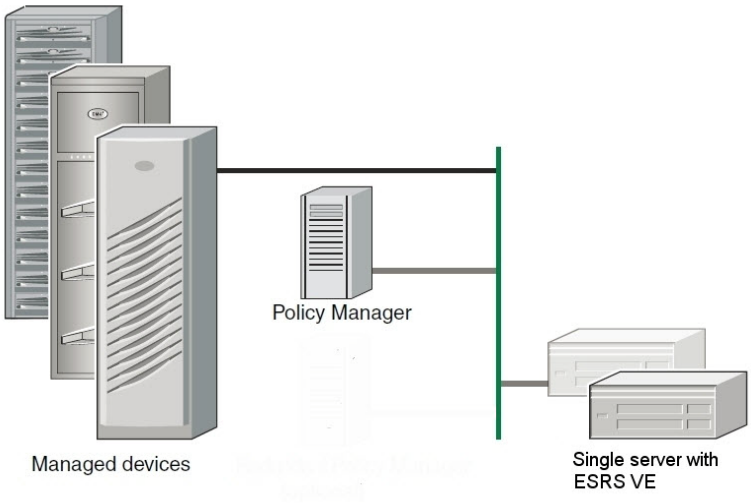


Figure 5 **Single ESRSv3 server and Policy Manager**

Note: ESRS is supported for use with any version of Policy Manager (2.02.1-xxx, 6.6, or 6.8).

The **Single ESRSv3 and Policy Manager** configuration shown on page 27 is designed for customers who initially want to utilize a single ESRSv3 server with a separate Policy Manager server.

Note: This configuration does not provide High Availability. It does, however, provide an upgrade path to a High Availability configuration.

The **Single ESRSv3 and Policy Manager** configuration has the following characteristics:

- **Number of required servers:** 2
- **Pro:**
  - Ease of upgrade from this configuration to a High Availability ESRSv3 Cluster configuration (the preferred configuration)
  - Permits easy recovery from a failed ESRSv3 server
- **Con:** Single point of failure for the server, which can negatively impact connect home and remote access

If you upgrade from the single ESRSv3 configuration to the High Availability ESRSv3 Cluster configuration, upgrade tasks will include installation of the new servers and ESRSv3 software. The new servers must be clustered to the original ESRSv3 server and pointed to the same Policy Manager. Devices should be configured to utilize the other servers in the cluster for connect home failover.

Note: ESRSv3 cannot be clustered with ESRS 2.x gateways or the ESRS device client.

Other supported configurations

EMC recommends one of the three configurations as described in "Recommended ESRS configurations" on page 26. However, EMC also supports the following configurations:

- High Availability ESRSv3 servers without Policy Manager
- Single ESRSv3 server without Policy Manager

This section provides details on these other supported configurations.

High Availability ESRSv3 servers without Policy Manager

The **High Availability ESRSv3 servers without Policy Manager** configuration shown in Figure 6 on page 28 is supported by EMC. The configuration has the following characteristics:

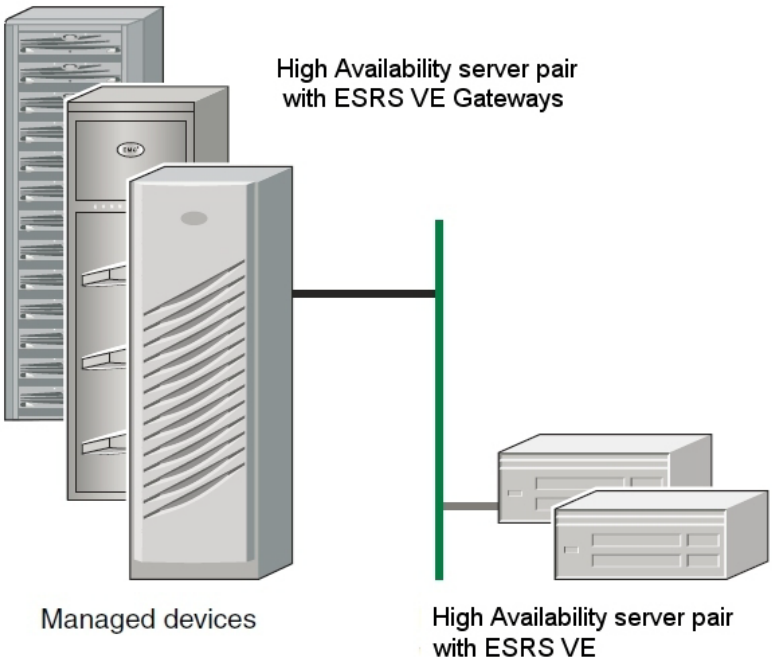


Figure 6 **High Availability ESRSv3 servers without Policy Manager**

- **Number of servers:** 2
- **Pros**:
  - This configuration can be upgraded to a High Availability ESRSv3 Cluster with standalone Policy Manager (preferred configuration).
  - This configuration provides connect home and remote support connection redundancy.
  - This configuration allows for easy recovery of the failed ESRSv3 server in the event of a server hardware failure.
- **Con**:

  No Policy Manager (therefore no access control or auditing).

If you decide to upgrade from this configuration to a configuration that includes a Policy Manager, installation and configuration will be required. Both ESRSv3 servers must be pointed to the new Policy Manager.

Note: ESRSv3 cannot be clustered with ESRS 2.x gateways or the ESRS device client.

Single ESRSv3 server without Policy Manager

The **Single ESRSv3 server without Policy Manager** configuration shown in Figure 7 on page 29 is supported by EMC.

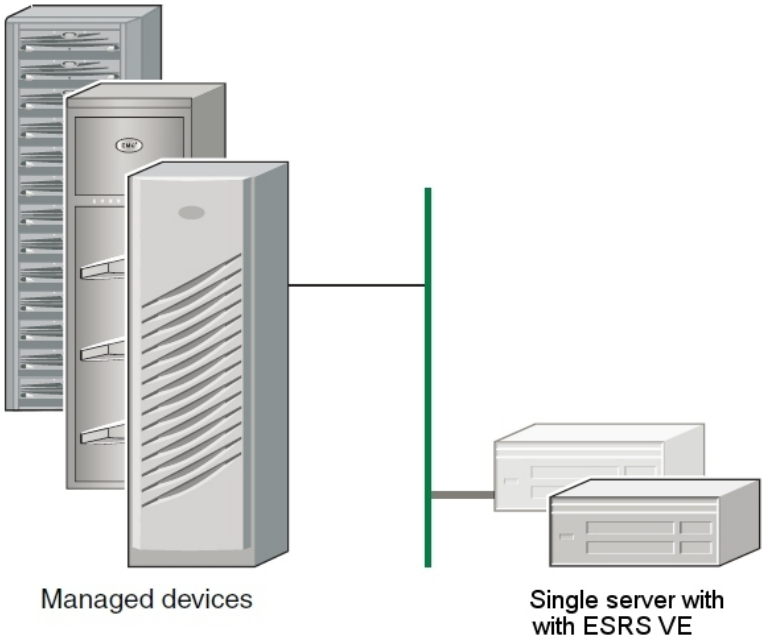


Figure 7 **Single ESRSv3 server without Policy Manager**

The configuration has the following characteristics:

- **Number of servers:** 1
- **Pro**:
  - This configuration can be upgraded to a recommended configuration.
- **Cons**:
  - No Policy Manager (therefore no access control or auditing)
  - Single point of failure for the ESRSv3 server

If you decide to upgrade from this configuration to a configuration that includes a High Availability ESRSv3 Cluster and a Policy Manager, upgrade tasks will include installation and configuration of the Policy Manager, installation of the new ESRSv3, and establishment of the High Availability ESRSv3 Cluster. The new ESRSv3 server must be clustered to the original ESRSv3 server, and both ESRSv3 servers must be pointed to the new standalone Policy Manager. All deployed devices must have connect home configured for failover to the new ESRSv3 server.

Note: ESRSv3 cannot be clustered with ESRS 2.x gateways or the ESRS device client.

Topology and network considerations

Follow the recommendations and other information in this section when you are making decisions about your site topology.

Determining the quantity of ESRSv3 and Policy Managers

The quantity of independent ESRS solutions you install is determined by the total number of devices that you want to monitor.

There is a maximum number of monitored devices that can be managed by a single ESRSv3 server (or HA clustered servers):

- A single ESRSv3 server (or a server in a High Availability cluster) can manage a maximum of 250 devices.
- A single Policy Manager can manage a maximum of 750 monitored devices.

Thus, for *each* 250 or fewer monitored devices, install one ESRSv3 server (or multiple clustered servers), and one Policy Manager per three ESRS servers (or three sets of clustered servers). Examples are shown in "Device limits" on page 24.

Note: For multi node devices, each node counts as a device.

Note: ESRS is supported for use with any version of Policy Manager (2.02.1-xxx, 6.6, or 6.8).

Note: ESRSv3 cannot be clustered with ESRS 2.x gateways or the ESRS device client.

Installing a separate Policy Manager server

EMC strongly recommends that you install the Policy Manager on a separate dedicated server on your internal production network.

This is recommended for the following reasons:

- **Easier access to the Policy Manager server**
  You will be able to quickly log in to the Policy Manager server to respond to a remote access request or make changes to your device access or authorization rules.
- **Increased network security for the Policy Manager**
  The Policy Manager is designed to be inaccessible to all third parties, including EMC. If you install the Policy Manager on a separate server inside your internal network, there is virtually no way for any third party to gain access to the server application.

Note: If you decide to place the Policy Manager in the DMZ, you must ensure that the Policy Manager has bidirectional access to your internal network so that it can provide email notification and permit access to the Policy Manager application.

Note: ESRS is supported for use with any version of Policy Manager (2.02.1-xxx, 6.6, or 6.8).

Protecting the ESRS server

There are no specific technical restrictions on the location of ESRSv3 servers within the network. However, you should do the following:

- Block all network ports that are not required by ESRSv3.

Note: Refer to the *ESRS Port Requirements* document to identify the ports that should be opened.

Using proxy servers

ESRS supports the use of a proxy server for routing outbound Internet traffic from the ESRSv3 to EMC. A list of tested proxy servers, protocols, and network configuration requirements is provided in Chapter 2, "Component Requirements."

When installing your ESRSv3 software, your EMC Global Services professional will configure the ESRSv3(s) to route all outbound Internet traffic to the proxy server and to use only the port that you specify to send data to the proxy server. The proxy server must direct the ESRSv3 transactions through the external firewall over port 443 and 8443.

Note: Port 8443 is not required for functionality, however without this port being opened, there will be a significant decrease in remote support performance, which will directly impact time to resolve issues on the end devices.

You are responsible for all proxy server configuration, rules, and troubleshooting needs resulting from ESRSv3 preparation, installation, and continued operation of the ESRSv3(s).

IMPORTANT

To ensure communication integrity, proxy servers and devices external to your DMZ must not perform any method of SSL decryption on outbound or inbound traffic for ESRS. SSL decryption performed on outbound communication by customer firewalls, proxies, Web traffic filtering appliances or cloud services, Web traffic shaping/load balancing, certificate verification, proxying, or Intrusion Detection Services (IDS) will cause a loss of connectivity to EMC.

Topology configurations

There are several options for locating the ESRSv3 and Policy Manager. This section provides details on several configurations.

The following topology diagrams represent a configuration of a High Availability ESRSv3 Cluster with a Policy Manager.

The recommended ESRS configuration is shown in Figure 8 on page 32. The ESRSv3 is located on a private management LAN (or VLAN), and the Policy Manager is located on the production network.

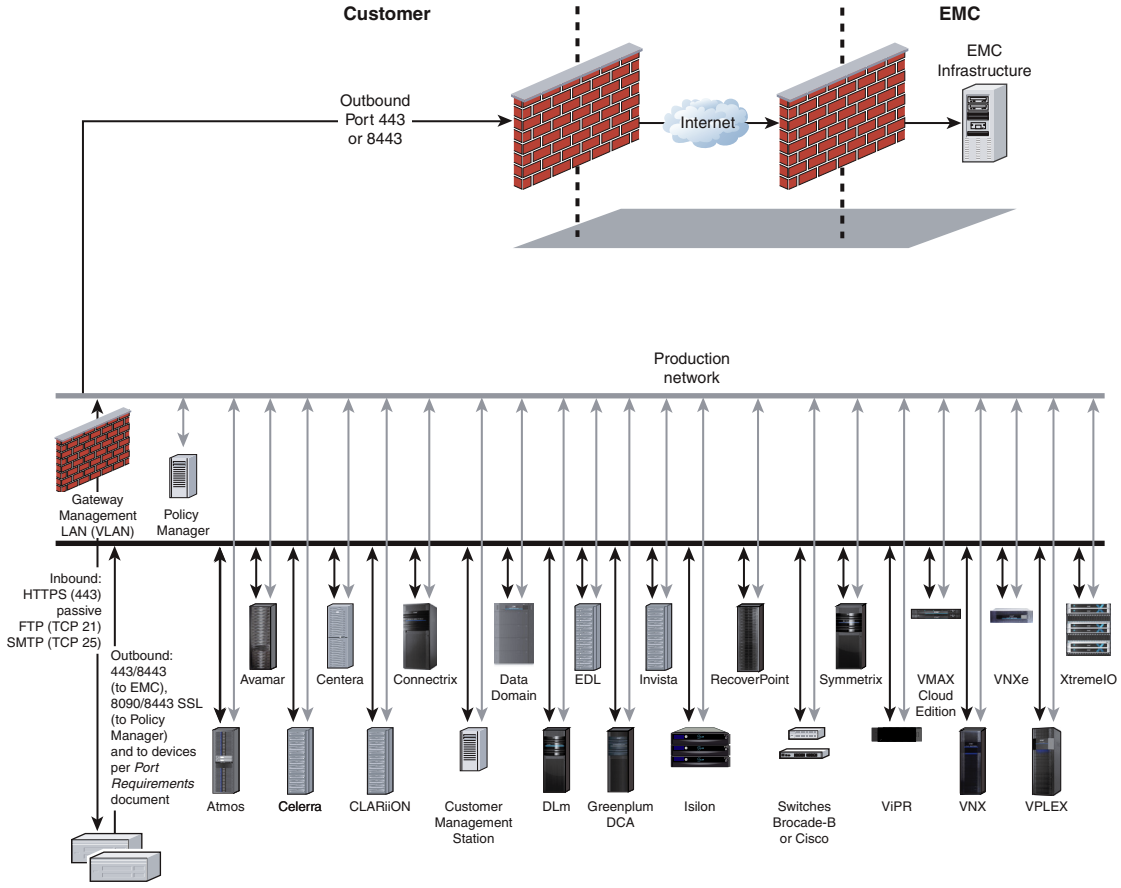


Figure 8 **ESRS/Management LAN configuration**

Note: ESRSv3 uses strict application IP and port mapping for connection to only the managed devices.

Another configuration is shown in Figure 9 on page 33. In this configuration, the ESRSv3 and Policy Manager are both located on your production LAN.

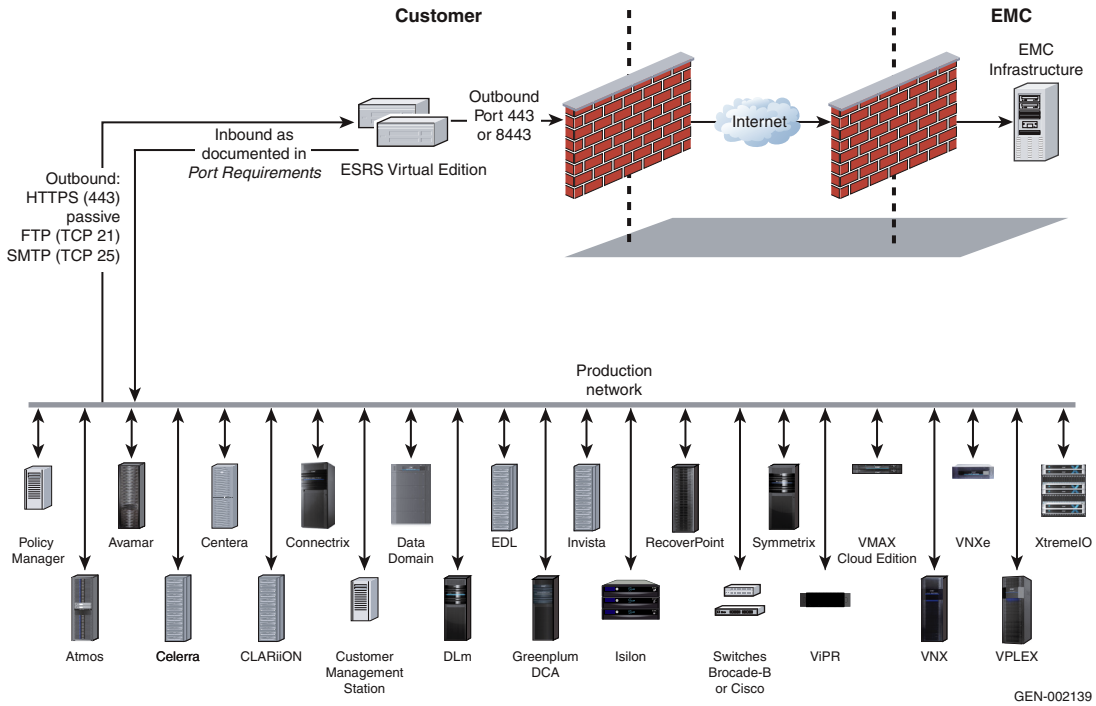


Figure 9 **ESRS/Production network configuration**

Note: ESRSv3 uses strict application IP and port mapping for connection to only the managed devices.

In Figure 10 on page 34, the ESRSv3 server is located in your DMZ, while the Policy Manager is located on your production network.

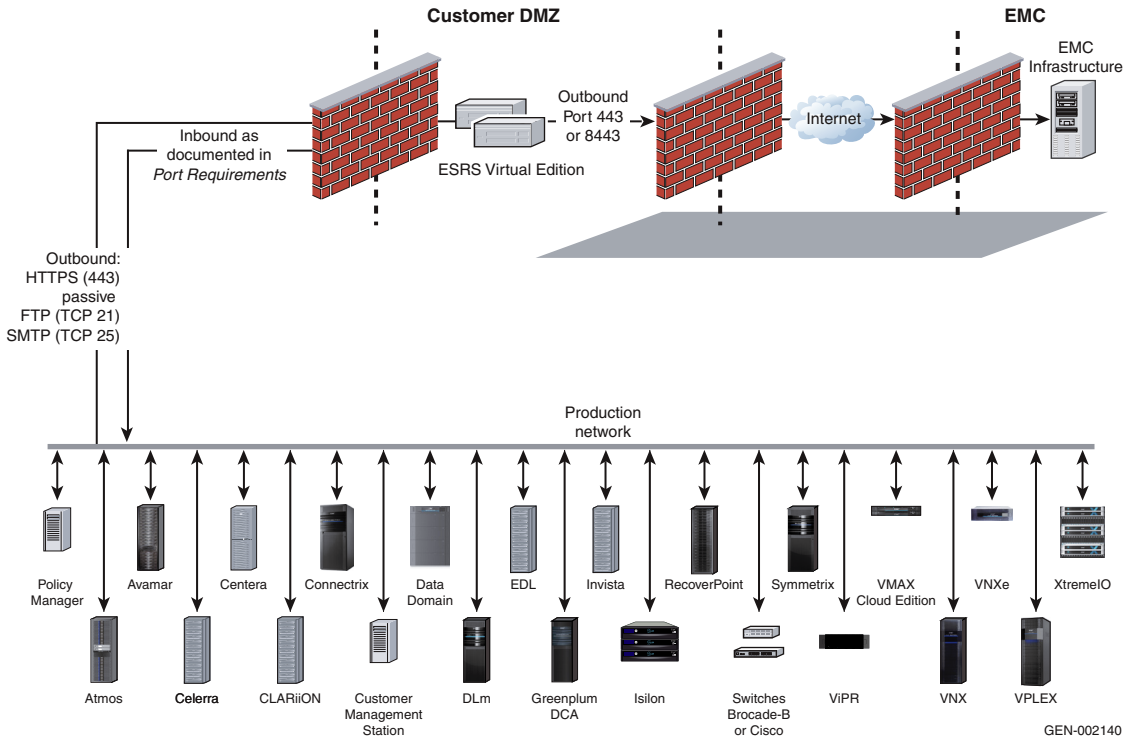


Figure 10 **ESRS/DMZ configuration**

Note: ESRSv3 uses strict application IP and port mapping for connection to only the managed devices.

Note: This configuration is the most difficult to configure and maintain. It is extremely dependent on customer network management. Unintended changes may have a significant impact on ESRS.

About the Policy Manager

The Policy Manager is the ESRS component that determines, for each access request, whether the request should be granted, denied, or forwarded elsewhere for a decision. The Policy Manager also creates and maintains audit logs for your site. These logs tell you which activities have occurred, when they occurred, and who performed them. If a service request is supplied as part of an access request, the Policy Manager will display the service request in the Notification email and in the audit of the request and approval or denial of the request.

Although a Policy Manager may be installed at any time, EMC recommends that it be installed at the time of the ESRS installation to ensure that the Policy Manager and ESRSv3 are linked.

IMPORTANT

Installation of a Policy Manager is *highly recommended*. Without a Policy Manager, your ESRS site will not have access control or audit logging, and access will be "Always Allow."

Policy Manager authorization settings

There are three levels of authorization for remote access activity. ESRS monitors activities and responds according to the authorization settings:

Always Allow — Use this setting if you want to always allow remote access for the activity.

Never Allow — Use this setting if you want to always deny remote access for the activity.

Ask for Approval — Use this setting if you want to require manual approval of remote access requests for the activity. Approval is performed by using the Policy Manager's web-based user interface.

Policy Manager failure

If the Policy Manager fails, certain default conditions apply. Some of these default conditions can be overridden. This section explains the default response and how to override the default response if desired.

Default response

If a Policy Manager server failure or communication failure occurs, policies are cached on the ESRS. The following default conditions will apply:

- An **Always Allow** or **Never Allow** policy setting will allow or deny the applicable activity request, just as the Policy Manager would have done.
- An **Ask for Approval** setting will time out, since the Policy Manager is not available to request and transmit approval. This will effectively deny the activity request.
- If a device is deployed while the Policy Manager is unavailable, the effective policy is Never Allow (Deny) until a valid policy is received.

About not using a Policy Manager

If you do not use a Policy Manager, or if the Policy Manager is not actively configured with the ESRSv3(s), ESRS approves all remote access requests and does not provide any access control audit logging.

High Availability ESRSv3 Clusters

To ensure maximum remote support uptime for your site, EMC strongly recommends that you prepare a minimum of two servers on which you or EMC Global Services can install an ESRSv3 for configuration as a High Availability Cluster.

Each ESRSv3 server in the High Availability eCluster should be running the same version of the ESRSv3 software. This will ensure that all of the ESRSv3 servers in the cluster are able to communicate with all of the device types qualified in that code release.

IMPORTANT

A High Availability ESRSv3 Cluster implementation provides multiple-server "active/active" server support. It does *not* perform an automated server failover. HA servers do not speak to each other.

Note: ESRSv3 cannot be clustered with ESRS 2.x gateways or the ESRS device client.

A High Availability ESRSv3 Cluster server configuration requires a minimum of two dedicated servers. These servers actively and simultaneously monitor devices on their shared managed device list. They also share the handling of remote access session requests and connect home requests based on the configuration of the managed devices.

With a High Availability implementation, your ESRSv3 servers implement an "active/active" solution, which eliminates the single-point-of-failure characteristic of a single-server configuration. The servers synchronize their managed device configuration information by relaying device list modifications to one another through the EMC ServiceLink application servers.

Devices are usually deployed and have Primary Connect Home configured to the ESRSv3 server that is physically located closest to the device. Event notification is performed by that ESRSv3, unless a problem occurs with that server. In that case, another server in the ESRSv3 Cluster performs the activity. Device monitoring for Support access connectivity is performed by ALL ESRSv3 servers in the cluster. Remote access session management is performed by the first ESRSv3 in the cluster that sends a heartbeat and responds to the access request.

High Availability ESRSv3 Cluster servers do not have failover

A High Availability ESRSv3 Cluster provides operational redundancy, ensuring that at least one of the servers is always operational. The High Availability cluster also provides backup capacity, which is operational in advance of any failure.

However, it is important to understand that ESRS does not implement *failover* behavior.

Note: General network failures that cause the loss of internet connectivity from your environment (i.e., independent / redundant paths to the Internet for each ESRSv3) result in ESRSv3 servers being unable to communicate with EMC and therefore will impact the ability of EMC to provide support.

Server failure in a High Availability ESRSv3 Cluster

If an ESRSv3 server fails, the other ESRSv3 servers in the cluster *already have* full responsibility. Also, when device-to-ESRSv3 ratios are properly configured, the other servers have the capacity for all device monitoring, event notification, and remote access session management.

When the failed server comes back online, all ESRSv3 once again simultaneously monitor devices and share the handling of connect home and remote access session requests.

Failover behavior at the EMC device level

Failover of connect home is initiated at an EMC storage device

When appropriately configured, EMC device connect home applications supports clustered High Availability servers as defined by the Product implementation of ConnectEMC. When an EMC device supported by ESRS recognizes that Connect Home calls cannot be received by the ESRSv3, it switches its Connect Home destination from its primary ESRSv3 to an alternate.

ESRSv3 configurations

EMC provides you with the option of configuring a single ESRSv3 server.

However, when you choose a single ESRSv3 configuration:

- You do *not* have High Availability protection. If the server fails, remote connection is not possible.
- If a server or connection fails and you have not enabled the failover connections, then EMC will not be notified of exception events on devices. As a result, EMC will not be able to provide remote support in a timely manner.

CHAPTER 4
Preparing for Site Installation

This chapter describes how to prepare your sites for installation of EMC Secure Remote Services (ESRS).Topics include:

- Overview 40

Additional information for specific information of Network; Operation System and ESRS application configuration are defined in:

- *EMC Secure Remote Services Installation Guide*
- *EMC Secure Remote Services Operations Guide*
- *EMC Secure Remote Support Policy Manager Release Operations Guide*

Consultation as to specifics may require contacting ESRS Customer Support.

Overview

This section provides information about site installation.

Coordination with EMC

Because EMC Secure Remote Services has several components, your network, storage system, and security administration personnel may choose to work closely with your EMC Global Services representatives to prepare your site for ESRS software installation.

As part of the software installation process, your EMC team may initiate multiple planning meetings with you to ensure that your onsite software installation is as fast and seamless as possible. You should also hold internal meetings to discuss your site configuration planning and documentation requirements.

For example, planning meetings could include the following meetings:

- An implementation kickoff meeting with your team and EMC Global Services and EMC Sales. This meeting would include a review of ESRS.
- A site configuration planning and documentation meeting with your network, storage, and security administration teams and EMC Global Services
- A final site installation planning and scheduling meeting with your network, storage, and security administration teams and EMC Global Services

Preparation work

In conjunction with your meetings with EMC, you should plan and execute the required preparation work. For additional details, see "EMC coordination schedule" on page 41.

EMC coordination schedule

Before installation of ESRS, you must gather or provide EMC Global Services with the following information for configuring your ESRS software:

- Contact information for the people who will prepare your site for installation and support your hardware and software
- Specifications for the servers on which you plan to install the ESRSv3 and Policy Manager applications
- Specifications for the number and types of devices to be managed by the Solution
- Specifications for the network configuration, network security policies, and Internet protocols that determine how devices, ESRSv3 and Policy Manager servers, and EMC's ServiceLink servers communicate with one another within ESRS

Note: A Pre-site Checklist is available from your EMC Global Services representative or may be downloaded from the Dell EMC Online Support Site (support.emc.com). The checklist will help you track and report the progress of your site preparation for ESRS.

Kickoff meeting

One of the first steps for a successful ESRS implementation is a review and implementation kickoff meeting with EMC Sales, EMC Global Services, or both.

At this meeting, you will:

1. **Review topology options** — The EMC team will provide an overview of the ESRS solution. You and the EMC team will discuss the possible site configuration options and review the necessary site requirements for your chosen configuration.
2. **Determine physical locations and resources** — You and the EMC team will identify physical locations for installing the ESRS and Policy Manager servers. You will identify the network, storage, and security personnel with in your organization responsible for:
   - Preparing your site for installation
   - Troubleshooting the customer-supplied hardware and software during installation
   - Maintaining the customer-supplied hardware and software after installation

   Note: EMC Global Services is not responsible for troubleshooting or resolving customer operating system or network issues. EMC Global Services is also not responsible for performing server operating system installation and configuration.

   - **Obtain EMC documentation and tools** — In addition to the *EMC Secure Remote Services Site Planning Guide*, EMC Global Services will provide you with the following documentation and tools:
     - EMC Secure Remote Services Release Notes
     - EMC Secure Remote Services Technical Description
     - EMC Secure Remote Services Pre-Site Checklist The checklist can be completed with EMC Global Service assistance.
     - EMC Secure Remote Services Port Requirements

- EMC Secure Remote Services Installation Guide
- EMC Secure Remote Services Operations Guide
- EMC Secure Remote Support Policy Manager Release 2.02.1-xxx Operations Guide
- EMC Secure Remote Services Policy Manager Release 6.6 Operations Guide

These documents and tools are also available for download from the Dell EMC Online Support Site (support.emc.com).

Action items

Begin your internal prep work — At this point, you should hold meetings with your network, storage system, and security administration teams. Review and be prepared to discuss the following items so that your team will be ready to make configuration decisions:

1. Review the following documents, as well as any additional information that EMC provides during the kickoff meeting:
   - *EMC Secure Remote Services Technical Description*
   - *EMC Secure Remote Services Site Planning Guide*
   - *EMC Secure Remote Services Port Requirements*
   - *EMC Secure Remote Services Installation Guide*
   - *EMC Secure Remote Services Operations Guide*
   - *EMC Secure Remote Services Policy Manager Operations Guide*
2. Decide which EMC devices that you want EMC to support remotely via ESRS IP. Chapter 1, "Overview" provides information on the device models that are available for support by the ESRS Solution.
3. Decide which ESRS site configuration option that you want to implement. Chapter 3, "Configurations" provides information to help you make this decision.
4. Decide how you want to configure your network to accommodate ESRS components. Chapter 3, "Configurations" provides information to help you make this decision.
5. Assign a resource to record the specifications of each component in your ESRS site configuration. Record the information in the *EMC Secure Remote Services Pre-Site Checklist* that you obtain from your EMC Global Services professional or by download from the Dell EMC Online Support Site (support.emc.com).

   This editable checklist will help you record information about whichever of the following components apply to your configuration:

   - ESRSv3 server
   - Policy Manager server
   - Managed devices
   - Proxy Server
   - Email server for Policy Manager
   - Email server for ESRSv3 (for failover Connect Homes, optional)
   - Network information for the connections between components

Note: Chapter 2, "Component Requirements" provides information on the minimum requirements for each customer-supplied component of ESRS.

6. Prepare a block diagram that depicts the planned server and device network configuration.

Configuration planning and documentation meeting

This will be the second meeting between your network, storage system, and security administration teams and EMC Global Services representatives. At this meeting, you will take the following actions:

1. **Review site plans** — You and your EMC Global Services representative will review and discuss your site configuration plans. You will use your completed *EMC Secure Remote Services Pre-Site Checklist* and block diagram as references.
2. **Create a prep-work schedule** — Your network, storage system, and security administration personnel will schedule the onsite pre-installation work that your teams must perform when setting up the ESRSv3 or Policy Manager servers. You should also review with EMC a schedule for the onsite time required for EMC to perform any other changes required before the upcoming ESRS installation.
3. **Schedule device upgrades (if needed)** — You should inform EMC Global Services whether any EMC device upgrades are needed to make them compatible with the ESRS solution.

Note: Any upgrades that must be performed on storage devices in order to make them compatible with ESRS are not part of the ESRS deployment process.

Action items

Implement site configuration — Your network, storage system, and security administration teams should now implement the server and network preparation work that they scheduled during the second meeting with EMC Global Services if applicable, as detailed in the following sections.

Installing and configuring servers

Before the ESRS software is installed, you must download and deploy the appropriate ESRS OVF/VHD or Docker Binary within your infrastructure and install and configure the required operating system for the Policy Manager servers.

Preparing network connections

Before running the ESRS software, you must ensure that firewall rules are in place so your ESRSv3 servers can communicate with EMC, with your Policy Manager server, and with your managed devices.

Configuring your network

To configure your network to support ESRS, take the following steps:

1. Ensure that your servers have unique addresses for all interfaces. Adhere to the following restrictions:

Note: All unused interfaces should be disabled.

- You must not use Port Address Translation. The ESRSv3 servers, as well as all EMC devices to be managed through ESRS, have services that listen for connection requests. These services will not work if Port Address Translation is employed.
- You must **not** use Dynamic IP (DHCP) addresses for any ESRS component, whether they are ESRSv3 servers, Policy Manager servers, or managed devices.

- If you use DHCP to assign IP addresses to any Solution components (ESRSv3 servers, Policy Manager servers, or managed devices), they must have "permanent reservation" IP addresses. Leases for any IP addresses that EMC devices are using must not expire. It is best to assign static IP addresses to those devices you plan to manage using ESRS.

2. Enable communication from each of your managed devices through your internal firewall to your ESRSv3 servers over the required port connections.

Note: EMC is not and will not be responsible for the configuration of Firewalls and or Router/Switch Access Control Lists (ACLs) or Proxy Servers.

Note: Applications or Devices that perform Web traffic monitoring and/or traffic shaping, Certificate Checking/Verification from public sources, or Proxying certificates have been known to cause connectivity issues especially for remote support connections. These devices must also be properly configured to permit ESRS traffic to pass unhindered.

Note: Intrusion Detection Systems (IDS) have also had similar effects on the solution and these devices or applications must also be properly configured to permit ESRS traffic to pass unhindered.

3. Follow these proxy server guidelines:

   - **If you are *not* using a proxy server for outbound Internet traffic:**
     Enable your ESRSv3(s) to communicate with the Internet through your external firewalls over ports 443 and 8443.
   - **If you *are* using a proxy server for outbound Internet traffic:**
     Enable your ESRSv3(s) to route all outbound traffic to the proxy server over the port required by your proxy server. The proxy server then needs to be able to connect outbound through the firewall over ports 443 and 8443.

   Note: Neither the proxy server nor the firewall should do SSL decryption. The customer is responsible for configuring the Proxy Server.

4. Check that you have no existing constraints on your network that could interfere with communication between the following:

   - ESRSv3 servers, EMC ESRS servers, and your managed devices

   To ensure connectivity, use the port listed in the *ESRS Port Requirements* document. These tables show which ports need to be open for ESRS network traffic.

Testing network connections and port functionality

You must test all required connectivity between the following pairs:

- ESRSv3 servers and EMC
- ESRSv3 servers and your outbound proxy server (if any)
- Your outbound proxy server (if you use one) and EMC
- ESRSv3 server and Policy Manager server (if applicable)
- ESRSv3 servers and managed devices

EMC requires that you test all of these connections *before* the Installation Planning and Scheduling meeting if applicable. You should take to that meeting a list of any problems or failures that you have encountered.

Installation planning and scheduling meeting

An installation and planning meeting should be the final meeting between customer network, storage, and security administration teams and EMC Global Services if requesting EMC assistance. At this meeting you should take the following actions:

1. **Review the Pre-site Checklist** — Your network, storage, and security administration teams should review your finalized pre-site checklist with EMC Global Services. The checklist must be complete and accurate since it will be used by EMC Global Services to perform ESRS installation. An editable Microsoft Word document is available for download from the Dell EMC Online Support Site (support.emc.com).
2. **Discuss and resolve problems** — Using your notes from network tests, your team should discuss with EMC Global Services any problems that must be resolved before scheduling the ESRS installation.

   Note that EMC Global Services is not responsible for:

   - Troubleshooting or resolving customer operating system or network issues
   - Performing server operating system installation and configuration
   - Configuring proxy servers or firewalls
3. **Schedule the installation** — Install or work with EMC Global Services to schedule your ESRS installation date.

APPENDIX A
ERS Version 3 connections to/from EMC products

This appendix describes the ESRS Version 3 (ESRSv3) connections to and from EMC products. It contains a list of the ESRSv3 GUI deploying suffixes that you need to choose for each product type.

- ESRSv3 GUI deployment suffixes..... 48

ESRSv3 GUI deployment suffixes.

Note: Refer to the *EMC Secure Remote Services Release Notes* for the latest information.

Table 4 on page 48 is a guide to how the EMC product at the customer and ESRSv3 at the customer communicate with each other. Refer also to the *EMC Secure Remote Services Port Requirements* document for specific protocols.

Where available, the recommended protocols for product connect-home are in order of preference:

1. HTTPS to ESRSv3 (preferred)
2. Email to ESRSv3
3. FTP to ESRSv3
4. Email via customer SMTP server to EMC (non-ESRS)

When deploying devices to ESRSv3 in the ESRSv3 GUI, you will need to choose deployment suffixes for each device type, as listed in Table 4 on page 48.

Table 4 ESRSv3 GUI deployment suffixes for each product type

EMC Product	ESRSv3 IP connection(s) to EMC Product	ESRS GUI Suffixes	Notes
Atmos	To management address on each node	-1 to -16	Use Node ID
Avamar	To the Utility Node management address	None	Use System ID for Serial Number Avamar CLI # mccli server show-prop | grep ID
Brocade	To management address for Departmental models. To Virtual address for Director models NOTE: Requires separate Windows monitoring workstation running CMCNE.	-CLI	To Switch management port (SSH)
		-CM	To CMCNE workstation (EMCRemote)
Caspian/Neutrino	To management address	-1 to -4	
Cellera	To Primary Control Station for all models. To Secondary and Active addresses for Dual Control Station models.	-P	Primary Control Station
		-S	Secondary Control Station
		-A	Active Control Station (Alias)
Centera	To minimum of two Access Nodes management address	-1 to -36	Node ID
Cisco	To switch management address NOTE: Requires separate Windows monitoring workstation running Cisco DCNM 5.x or higher	None	To Switch management port (SSH)
CLARiiON	To both SPA and SPB management addresses NOTE: Requires separate Windows monitoring workstation running ESRS VNX IP Client	-A	Storage Processor A
		-B	Storage Processor B

Table 4 ESRSv3 GUI deployment suffixes for each product type

EMC Product	ESRSv3 IP connection(s) to EMC Product	ESRS GUI Suffixes	Notes
CloudArray	Refer to CloudArray Install Documentation	-MGT	Management Station
		-BMC	baseboard management controller
		-IDRAC	
CloudBoost	Do not deploy in ESRSv3 GUI		Deploy from CloudBoost
Customer Management Workstation	To Management workstation	-1 to -32	Management Workstation ID
Data Domain	To appliance management address	None	Appliance
DL3D	To appliance management address	-1 to -3	Appliance
DLm	To Primary, Secondary and Active management addresses	-P	Primary Control Station
		-S	Secondary Control Station
		-A	Active Control Station (Alias)
DLm3	To Primary, Secondary and Active management addresses	-ACP1	Primary Access Control Point
		-ACP2	Secondary Access Control Point (for Dual ACP only)
		-ACPA	Active Access Control Point (Alias for Dual ACP only)
DLm4	To VTE1, VTE2 and Active VTE management addresses	-VTE1	Primary Virtual Tape Engine
		-VTE2	Secondary Virtual Tape Engine
		-VTEA	Active Virtual Tape Engine (Alias)
DPA	Do not deploy in ESRSv3 GUI		Deploy from DPA
DPAppliance	Refer to product documentation	-ACM	
DPC	Do not deploy in ESRSv3 GUI		Deploy from DPC
ECS	To management address of each VIPR virtual machine. To public address of one ECS node	-AT	ECS Node
		-SW1	VIPR virtual machine 1
		-SW2	VIPR virtual machine 2
		-SW3	VIPR virtual machine 3
EDL	To Engines, SPA and SPB management addresses	-A	Engine A Service IP
		-B	Engine B Service IP
Embeded NAS (eNAS)	To appliance management address	None	Appliance
Greenplum DCA	To management interface	-B	Backup Node
		-P	Primary Node

Table 4 ESRSv3 GUI deployment suffixes for each product type

EMC Product	ESRSv3 IP connection(s) to EMC Product	ESRS GUI Suffixes	Notes
Invista	To appliance management address	-A	Management addresses
		-B	
Isilon	To dedicated Management Subnet address for each node	None	Connect to individual node
PowerPath	Do not deploy in ESRSv3 GUI		Deploy from PowerPath
RecoverPoint	To each physical appliance address and one management address per cluster NOTE: Use Software Serial ID as the serial number for all entries including nodes. Admin CLI # get_system_settings	-16	Cluster management address
		-1 to -15	Physical Node ID and Physical node management address
ScaleIO	Do not deploy in ESRSv3 GUI		Deploy from ScaleIO
Symmetrix VMAX	To Service Process management address	None	Service Processor
Symmetrix VMAX3	To primary and secondary MMCS addresses	-MMCS1	Management Module Control Station 1
		-MMCS2	Management Module Control Station 2
Unity/UnityVSA	To appliance management address	None	Appliance
VCE Vision	Do not deploy in ESRSv3 GUI		Deploy from VCE Vision
ViPR	To each ViPR management address	-1 to -3	Virtual Machine 1 to 3
ViPR SRM	Do not deploy in ESRSv3 GUI		Deploy from ViPR SRM Interface
VNX Block	Both SPA and SPB required NOTE: Requires BLOCK OE 05.32.000.5.215 or higher (VNX1) and 05.33.000.5.072 or higher (VNX2)	-BLOCKA	Storage Processor A
		-BLOCKB	Storage Processor B
VNX Unified	To Primary, Secondary, Active Control Station addresses. To SPA and SPB management addresses	-FILEP	Primary Control Station
		-FILES	Secondary Control Station
		-FILEA	Active Control Station (Alias)
VNXe	To management address	None	
VPLEX	To management address	None	Appliance
VxRail (VSPEX BLUE)	Do not deploy in ESRSv3 GUI		Deploy from VxRail (VSPEX BLUE)
XtremIO	To management address	None	Appliance

Note: Some products only send product-specific information to EMC, and do not connect-home for alerts/configuration files etc.

GLOSSARY

This glossary contains terms related to remote services and ESRS.

A

access See *Remote Access*.

C

connect home Connecting from a remote site to EMC's support network.

D

DMZ Demilitarized zone — Device used to secure an internal network from unauthorized external access.

Dynamic IP address An address that is assigned by the access device by which the user's host connects over a dialup telephone line or by a set-top box for an IP over cable network.

E

Dell EMC Online Support Site Web-based access on support.emc.com to documentation, downloads, and support information for EMC customers and internal EMC users.

ESRS EMC® Secure Remote Services is an IP-based automated connect home and remote support solution enhanced by a comprehensive security system. ESRS creates both a unified architecture and a common point of access for remote support activities performed on your EMC products.

ESRS Virtual Edition EMC Secure Remote Services, Virtual Edition, which is installed on an ESX or Hyper-V Server, acts as the single point of entry and exit for all connect home and remote support activities.

F

failover The capability to switch over automatically to a standby server upon the failure or abnormal termination of the previously active server. Failover happens without human intervention and generally without warning.

firewall A hardware or software device that is configured to permit, deny, or proxy data through a computer network which has different levels of trust.

FTP File Transfer Protocol — Used to transfer data from one computer to another, over the Internet or through a network.

G

Gateway 2.x An ESRS 2.x software component that is installed on a customer-supplied dedicated server (or servers) or VMware instance. The servers act as the single point of entry and exit for all IP-based EMC remote notification and remote support activity.

P

Policy Manager An ESRS software component that is installed on a customer-supplied server or servers. It enables customizable control of remote access to customer devices and maintains an audit log of remote connections.

proxy server A server (a computer system or an application program) which services the request of its servers by forwarding request to other servers. A server connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server provides the resource by connecting to the specified server and requesting the service on behalf of the server. A proxy server may optionally alter the server's request or the server's response, and sometimes it may serve the request without contacting the specified server.

R

remote access Communication with a processing device from a remote location through a data link.

S

SMTP Simple Mail Transfer Protocol — The de facto standard for email transmissions across the Internet.

T

topology Network configuration, including firewalls, servers, devices, and ports used for communication between all devices.

Transport Layer Security (TLS) port A port that uses cryptographic protocols to provide secure Internet communications for data transfers.

INDEX

A
AES encryption 11
architecture 10
Atmos 12, 48
authorization settings 35
Avamar 12, 48

B
Brocade 48
Brocade switches 13
browser requirements 18

C
Caspian 12
Caspian/Neutrino 48
Celerra 12
Cellera 48
Centera 12, 48
Cisco 48
Cisco switches 13
CLARiiON 12, 48
CloudArray 12, 49
CloudBoost 12, 49
configurations 23
    network 43
    recommended 26
    supported 28
connect home 20
connectivity testing 44
CPU requirements 18
Customer Management Workstation 49
customer responsibilities 14

D
Data Domain 12, 49
Data Protection Advisor (DPA) 12
device limits 24
device upgrades 43
devices supported 12
devices, maximum number 30
DHCP 19
Disk Library (EDL) 12
DL3D 49
DLm 12, 49
DLm3 49
DLm4 49
Docker 10, 11, 14, 24
DPA 12, 49
DPC 49
DSSD 12
dynamic IP addresses 43

E
eCDM 13
ECS 13, 49
EDL 12, 49
Elastic Cloud Storage (ECS) 13
Embedded NAS (eNAS) 13
Embeded NAS (eNAS) 49
EMC responsibilities 14
Enterprise Copy Data Management (eCDM) 13
environment 12
ESX Server requirements 18

F
failover 36
free disk space requirements 18

G
Greenplum DCA 13, 49

H
High Availability Gateway Clusters 36
HTTP 20
HTTPS 20

I
installation 40
Invista 13, 50
IP addresses, dynamic 19
Isilon 13, 50

M
meetings
    configuration planning and documentation 43
    installation planning and scheduling 45
    kickoff 41
memory requirements 18

N
Network Address Translation 19
Network requirements 18
networks
    configuring 43
    connections, testing 44
    ports, blocking 30
    requirements 18
Neutrino 12, 48

P
people resources, identifying 41
physical locations, determining 41

planning meetings See meetings 40
Policy Manager 11, 30, 35
    failure 35
    redundant 11
policy settings 35
Port Address Translation 19
port diagram 21
PowerPath 13, 50
prep-work schedule 43
Pre-site Checklist 41, 45
proxy servers
    enabling 19
    guidelines 44
    protocols 20
    tested 20
    using 31

R

RecoverPoint 13, 50
Redundant Policy Manager 11
remote access 35
requirements
    browser 18
    CPU 18
    ESX server 18
    Free disk space 18
    memory 18
    network 18
    networks 18
    server requirements 18
responsibilities
    customer 14
    EMC 14

S

ScaleIO 13, 50
server requirements 18
servers
    requirements, hardware and OS 18
    types of 18
single ESRS server 37
site installation 40
site planning process 14
site plans 43
supported devices 12
Symmetrix 13
Symmetrix VMAX 50
Symmetrix VMAX3 50

T

testing network connections 44
testing, connectivity 44
TLS 14, 19, 20, 52
topology 30, 31, 32, 33, 34, 41
Transport Layer Security (TLS) 14, 19, 20, 52

U

Unity 13, 50
UnityVSA 13, 50

V

VCE Vision 13, 50
ViPR 13, 50
ViPR SRM 13, 50
VNX 13
VNX Block 50
VNX Control Station 13
VNX Unified 50
VNXe 13, 50
VPLEX 13, 50
VSPEX BLUE 13, 50

X

XtremIO 13, 50