Network requirements

The following ports are used by the various vCommander components. You configure some of these ports during installation, and you can also configure ports after installation using the vCommander Control Panel. Certain ports can be configured only through a system property; for more information, contact support@embotics.com.

IMPORTANT: To protect the security of the vCommander system, all ports must be firewalled, with the exception of ports that are required to be inbound.

✏️ Where the direction is outbound, this implies a corresponding inbound connection to the target.

Table: Network Requirements - Basic Operations

Connection	Ports	Protocol	Direction	Description
vCommander Webserver	443	TCP	Inbound	Access to vCommander admin console, Service Portal and REST API
vCommander Microsoft SQL Server	1433	TCP	Outbound	Access to the vCommander database. Additional ports may be required depending on the configuration of your SQL server
vCenter	443	TCP	Outbound	Communications with individual vCenters or their external Platform Services Controllers
vCenter Hosts	443	TCP	Outbound	Access to the vCenter hosts for VM Guest OS file copy operations
Amazon Web Services	443	TCP	Outbound	Communications with Amazon Web Services API
Microsoft Azure	443	TCP	Outbound	Communications with Microsoft Azure API
Windows Guest OS Features	135 139 445	TCP	Outbound	Access to Windows VMs for issuing WMI commands and file copy operations
Linux Guest OS Features	22	TCP	Outbound	Access to Linux VMs for issuing SSH commands

©2017 All rights reserved in all media

Connection	Ports	Protocol	Direction	Description
Datastore Scanning	443	TCP	Outbound	Access to VMware hosts through HTTPS to collect file layout
Legacy Datastore Scanning	22	TCP	Outbound	Access to VMware hosts through SSH to collect file layout. Only used when HTTPS access is not available

Table: Network Requirements - Authentication

Connection	Ports	Protocol	Direction	Description
Kerberos Key Distribution Center	88	TCP	Outbound	Access to authenticate against an Active Directory or LDAP server
Active Directory Domain Controller for Remote LDAP Traffic	389	TCP UDP	Outbound	Access to authenticate against an Active Directory or LDAP server
Active Directory Domain Controller for Remote Global Catalog Traffic	3268	TCP	Outbound	Access to query the global catalog of an Active Directory or LDAP server
Active Directory Domain Controller for Remote Secure LDAP Traffic	686	TCP	Outbound	Access to authenticate against a secure Active Directory or a secure LDAP server
Active Directory Domain Controller for Remote Secure Global Catalog Traffic	3269	TCP	Outbound	Access to query the global catalog of a secure Active Directory or secure LDAP server

Table: Network Requirements - Optional

Connection	Ports	Protocol	Direction	Description
Splunk Server	8089	TCP	Outbound	Communications with Splunk server for retrieval of guest OS performance metrics

©2017 All rights reserved in all media

Connection	Ports	Protocol	Direction	Description
BlueCat™ Server	80	TCP	Outbound	Communications with BlueCat™ IP address management server for addressing assignments

Table: Network Requirements - Client Connections

All of these connections go from the client browser to the respective servers.

Connection	Ports	Protocol	Direction	Description
VM Access (Remote Desktop)	3389	TCP	Inbound	Access to remote control VMs using RDP
VM Access (Virtual Network Computing)	5900	TCP	Inbound	Access to remote control VMs using VNC
VMware Console - WebMKS (HTML5)	9443 (vCenter 6.0) 7343 (vCenter 5.5)	TCP	Inbound	Access to remote control VMs using WebMKS Console
VMware Console - Plug-in	443 (vCenter) 902 (ESX)	TCP	Inbound	Access to remote control VMs using VMware Remote Console (VMRC) Plug-in

Table: Network Requirements – Advanced Configuration

Connection	Ports	Protocol	Direction	Description
VM Access Proxy Appliances – Web Server	443	TCP	Inbound	Publishing listener for WebMKS open console sessions
VM Access Proxy Appliances – Web Server	8443	TCP	Inbound	Publishing listener for RDP, VNC, SSH and plug-in-based open console sessions
Service Portal Appliances – Database Connection	1433	TCP	Outbound	Access to the vCommander database for distributed Service Portal nodes. Additional ports may be required depending on the configuration of your SQL server

©2017 All rights reserved in all media

Connection	Ports	Protocol	Direction	Description
vCommander Authentication Service	8042	TCP	Inbound	Communications with distributed Service Portal nodes
Highly Available vCommander Heartbeat	443	TCP	Bidirectional	Passive node access to check health of active node
VM Access (Hyper-V Console)	2179	TCP	Outbound	Access to remote control VMs using the Hyper-V console

Guest OS Scanning Port Requirements

Guest OS scanning of Windows VMs also requires firewall rules to handle a dynamic range of ports opened for the response when vCommander queries the VMs on TCP port 135. To avoid opening a large range of high ports, please refer to the following Knowledge Base articles for instructions on how to configure the Windows Firewall to enable these ports:

- Configuring Windows for Guest OS Scans Using Group Policy
- Configuring Windows for Guest OS Scans

Account on each managed system

vCommander requires an administrative account on each managed system. The account must have full administrative access on the entire managed system. Administrator privileges are required for a number of functions that vCommander performs. These functions include retrieving VM and infrastructure information, managing VM identity, powering VMs on and off, and other policy actions.

Embotics® recommends that you create a uniquely identifiable administrative account on each managed system (for example, Embot). Creating a unique account name allows you easily to track vCommander commands sent to the managed system by vCommander or by vCommander users.

vCommander does not make use of VMware's Linked Mode feature. vCommander communicates with each vCenter directly.

Third-party integrations

The following table provides a list of third-party software that can be integrated with vCommander, including supported versions where applicable.

Table: Third-Party Integrations

Integration Category	Supported Systems and Protocols	Integration Type
Authentication	Active Directory®	Bundled
	LDAP	Bundled
	SAML2 WebSSO	Bundled
	Windows SSO	Bundled

©2017 All rights reserved in all media

Integration Category	Supported Systems and Protocols	Integration Type
Configuration Management and Application Deployment / Automation	Chef™ 12.15.7	Bundled
	Puppet™ Enterprise 2017.1.1	Bundled
	SCCM 2012 R2	Scripted
	Jenkins CI with PowerShell plug-in	Scripted
	ServiceNow or ServiceNow Express, with REST API access	Scripted
	Zerto Virtual Manager (ZVM) Replication 4.5u1 (vCenter only)	Scripted
	Docker 1.11.2	Scripted
	vCommander REST API plus Windows Task Scheduler (and similar)	Scripted
	vCenter metadata synchronization, for all vCenter versions supported by vCommander	Scripted
IPAM	BlueCat™ IPAM 4.1	Bundled
Application Monitoring	Splunk® 6.2, 6.1 (with HTTPS protocol)	Bundled
Notification	SNMP 2	Bundled
	SMTP	Bundled
Backup	Veeam Backup & Replication 8.0	Additional download required
Workflow Automation	vCommander REST API client for PowerShell 4, 3 with .NET Framework 4.5 or higher	Additional download required

Scaling Embotics® vCommander® Hardware Requirements

Embotics® vCommander® connects to one or more hypervisors to provide powerful automation and reporting options, with a better user experience for producers and consumers of virtual services. This tight integration with your virtual infrastructure means that the hardware requirements for vCPUs, memory and disk space scale in lockstep with your virtual infrastructure's rate of occupancy and activity. Use the guidelines in this section to establish a good starting point for your installation, and be prepared to allocate more resources over time as your virtual infrastructure grows.

See also the Knowledge Base article Migrating the Embotics® vCommander® Application, which covers migration of vCommander and its database.

©2017 All rights reserved in all media