This document details critical network ports required for VMware vRealize Automation (vRA) and Ansible to securely communicate from a trusted zone into a DMZ. It categorizes ports by product, operating system, and necessity, covering key protocols such as SSH, WinRM, and HTTPS.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Product | Port | Protocol | Traffic Direction | OS | Used For | Needed | Comment |
| vRA | 443 | TCP | Trusted → DMZ | Both | HTTPS communication between vRA components and endpoints (API, UI, agents) | Mandatory | Core secure channel; must be open for all vRA service communication |
| vRA | 22 | TCP | Trusted → DMZ | Linux | SSH access to Linux agents or endpoints | Mandatory | SSH access for Linux guest agent deployment and management |
| vRA | 135 | TCP | Trusted → DMZ | Windows | Windows RPC for IaaS Windows agents | Mandatory | Required for Windows agent communication; high security risk — consider jump hosts or firewall ACLs |
| vRA | 139 | TCP | Trusted → DMZ | Windows | SMB for Windows file shares and agent deployment | Mandatory | Used by Windows guest agents; SMB over DMZ is risky, recommend tunneling or agentless approaches |
| vRA | 445 | TCP | Trusted → DMZ | Windows | SMB over TCP for Windows agent file operations | Mandatory | Same risks as above; critical for agent deployment, restrict heavily |
| vRA | 5480 | TCP | Trusted → DMZ | Both | vRA Appliance management UI (vAMI) | Optional | Appliance admin UI port; restrict access to trusted admins only |
| vRA | 80 | TCP | Trusted → DMZ | Both | HTTP fallback or redirect to HTTPS | Optional | Should be blocked if HTTPS strictly enforced; used only for redirecting traffic |
| Ansible | 22 | TCP | Trusted → DMZ | Linux | SSH to target hosts for Linux/Unix configuration | Mandatory | Default and primary port for Ansible management |
| Ansible | 5986 | TCP | Trusted → DMZ | Windows | WinRM HTTPS for secure Windows remote management | Mandatory | Recommended WinRM port; encrypted communication for Windows hosts |
| Ansible | 443 | TCP | Trusted → DMZ | Both | HTTPS for REST APIs or custom modules | Optional | Needed if Ansible workflows use API calls or plugins requiring HTTPS |
| Ansible | 53 | UDP/TCP | Trusted → DMZ | Both | DNS queries | Optional | Required if hosts or services inside DMZ need DNS resolution; can be internal or forwarded |
| Ansible | 5985 | TCP | Trusted → DMZ | Windows | WinRM HTTP for Windows remote management | Optional | Non-encrypted WinRM; only use if HTTPS unavailable and in secure environments |
| Ansible | 123 | UDP | Trusted → DMZ | Both | NTP (Network Time Protocol) for time synchronization | Optional | Important for time sync especially in Kerberos environments; often overlooked but critical |

|  |  |  |
| --- | --- | --- |
| Product | Source Description | URL |
| vRA | VMware vRealize Automation 8.x Port Requirements | <https://docs.vmware.com/en/vRealize-Automation/8.13/com.vmware.vra.install.doc/GUID-5B89C6A7-CBA9-4B44-8D81-77E4E56D17E0.html> |
| vRA | vRealize Automation 7.x Ports and Protocols | <https://docs.vmware.com/en/vRealize-Automation/7.6/com.vmware.vra.install.doc/GUID-B6E7D010-332D-41EF-9EDC-430D1A8CEBD6.html> |
| vRA | VMware Knowledge Base: Ports Used by vRA | <https://kb.vmware.com/s/article/2147376> |
| Ansible | Ansible Official Documentation - Connection Details | <https://docs.ansible.com/ansible/latest/user_guide/connection_details.html> |
| Ansible | Ansible Windows Setup and WinRM Ports | <https://docs.ansible.com/ansible/latest/user_guide/windows_setup.html#setting-up-winrm> |
| Ansible | Microsoft Documentation - WinRM Network Ports | <https://learn.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management> |