



# Configuration Planning and Installation Guide

Version 8.2.7

Copyright 2020 NComputing Global, Inc. All rights reserved. Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photo copying and recording for any purpose other than the purchaser's personal use without the written permission of NComputing Global, Inc. VERDE, NComputing, and the NComputing logo are trademarks of NComputing Co., Ltd. Other company, product, or service names may be trademarks or service marks of others. NComputing Global, Inc.

400 Concar Drive, 4<sup>th</sup> Floor, San Mateo, CA 94402

Phone: 1.650.409.5959

Fax 1.650.409.5958

# Table of Contents

Introduction .....	4
Planning the Installation .....	5
Server Capacity Planning .....	5
Shared Storage Planning .....	9
Sizing Per Desktops .....	10
Network Planning for Client Access .....	12
Guest Image RAM and Disk Space Planning .....	14
Supported Platforms .....	15
Multiple Methods of Installation .....	20
VERDE installed on bare metal server (VERDEOS) .....	20
VERDE installed on non-bare metal server (RPM method) .....	20
Common Installment Requirements .....	21
VERDE Hosting .....	21
Clustering Requirements .....	22
Upgrading VERDE Requirements .....	22
Installing VERDEOS .....	23
Installation Steps .....	23
Installing the VERDEOS Package .....	24
Installing VERDE Using RPMs .....	29
Considerations .....	29
Configuring VERDE using the RPM Method .....	30
Installing the VERDE RPMs .....	34
Configuring Isolated Gateway Servers .....	47
Index .....	51

## Introduction

This guide is designed to provide you with the multiple installation options available for creating a working VERDE 8.2.7 system. VERDE 8.2.7 requires a bare-metal installation on physical hardware for its desktop hosting. Certain other elements may be run from within a virtual machine. It is up to the systems administrator to determine which of the installation paths work best for the IT environment hosting the VERDE server(s).

The installation choice is up to you. This guide contains instructions for both methods, VERDEOS or RPM based. Please refer to the section below that applies to your installation preference:

- Installing VERDEOS on p. 23
- Installing VERDE Using RPMs on p. 29



<b>CHAPTER 4</b>	<b>33</b>
VERDE Management Console	33
Starting the VERDE Management Console	35
Setting General Configuration Parameters	36
Administration	40
Managing Directory Users and Groups	46
Gold Images Overview	50
Managing Session Settings	51
VERDE Virtual Application Layers	61
Organization Overview	64
Assign MAC Address Pools	69
Managing Desktop Pools	70
Managing Desktop Policy	72
Computer Resources	77
Managing Debug Logs and Events	79
<b>CHAPTER 5</b>	<b>80</b>
Installing a Gold Image Virtual Machine	80
Windows Gold Image Considerations	81
Windows RDP Access and Group Policy	81
Branch Servers and Gold Images	82
Single Sign-on and Active Directory in a Gold Image	82
Gold Images	83
Preparing to Install a Gold Image Operating System	87
Installing a Windows Server 2008 R2 Gold Image	88
Installing Windows Server 2012 Gold Image	90
Installing a Windows 7 Gold Image	93
Installing a Windows 8.1 Gold Image	95
Installing a Windows 10 Gold Image	97
Installing a Linux Desktop Gold Image	99
Making Changes to a Gold Image	102
Upgrading Gold Image Guest Drivers	106
Upgrading and Importing Gold Images	108
<b>CHAPTER 6</b>	<b>109</b>
Configuring the Gold Image	109
Windows Activation Tasks	111
Windows Advanced Configuration	112

## Planning the Installation

### SERVER CAPACITY PLANNING

It is critical for the server to have enough resources to accommodate **peak concurrent virtual desktop usage**, which is not necessarily the same as peak connected usage. Any virtual desktop environment running on the server—whether a user is connected to it or not—counts toward concurrent usage. Even if users are not connected to the server, they might still have a virtual desktop environment, consuming resources.

When planning for adequate server capacity in an existing environment, there are two factors to consider:

- the density of the VERDE virtual server desktop
- the components that make up local storage

The total assigned virtual machine RAM plus overhead should never exceed the amount of physical RAM in the server. Doing so will result in extreme performance degradation.

### CALCULATING VERDE SERVER VIRTUAL DESKTOP DENSITY

To determine the virtual desktop density possible on particular hardware for a VERDE Server, gather the following information:

- Number of CPU sockets (C)
- Number of CPU cores per socket (c)
- Total system RAM in GB (M)
- Guest virtual machine RAM assignment in GB (m)

#### Memory Considerations

The number of concurrent sessions that fit in memory on a particular VERDE Server (T1)—that is, sessions that are either connected or disconnected—can be calculated as follows:

$$T1 = ((M - 8 \text{ GB}) / (m + 0.128 \text{ GB}) * .80)$$

The actual applications running in guest virtual machines play a major role in determining the virtual desktop density of a given VERDE Server. For example, office/business applications scale better than high-resolution multimedia programs.

Virtual machine RAM assignment must be calculated for capacity, not performance. Unlike with a physical computer, assigning more RAM to a virtual machine does not improve performance. Assigning too much RAM to a virtual machine might degrade performance by reducing the amount of system-wide caching that the host can perform.

The allocation of RAM must be based on the minimum RAM required to run applications. Most application vendors provide a “minimum” and a “recommended” RAM requirement. When planning virtual machine RAM assignment, use the “minimum” requirement. If necessary, assign less than the minimum to increase server density.

Allocate up to 8 GB of RAM for VERDE system software. Add this amount of RAM to the required guest RAM calculation or subtract it from the total system RAM to accurately determine the number of concurrent sessions possible.

Allocating more memory than the minimum 8 GB will improve performance significantly. Any additional memory is used to cache Gold Images into memory. NComputing Global, Inc. recommends that up to 20% of total system memory is allocated to cache I/O memory. To calculate for this, add to the 8 GB minimum in the formula to reflect up to 20% of total system memory.

For example, with 92 GB of RAM and 1 GB per session, the number of concurrent sessions that can fit in memory is 60:

$$T1 = ((92\text{GB} - 8\text{GB}) / (1\text{GB} + 0.128\text{GB}) * .80)$$

### CPU Considerations

A common guideline or metric for calculating the number of concurrent sessions that can be executed on a given CPU core is 8. Depending on the application profile, this number might be as high as 15 (or more). For typical application load (office/productivity applications), it is safe to use 8 concurrent sessions per core metric. To calculate the maximum number of concurrent sessions that can be run on a given VERDE Server without degrading session performance (T2):

$$T2 = 8 \times C \times c$$

For example, on a system with two sockets and four cores per socket:

$$T2 = 8 \times 2 \times 4$$
$$(T2 = 64)$$

### Putting it Together

The actual maximum number of concurrent sessions that will both fit in memory and execute with expected performance on a given VERDE Server (T) is the lesser of the values T1 and T2. In the examples above, this number would be T = 64.



## LOCAL STORAGE PLANNING

Traditional VDI requires excess amounts of high performance storage, which is costly to purchase and complex to manage.

VERDE Storage Optimizer™ cache I/O technology works by caching the Input/Output Operations per Second (IOPS) from each virtual desktop onto VDI compute nodes for common data reads and transient data writes. VERDE replicates shared virtual desktop data at scheduled intervals, while running virtual desktop workloads from the VERDE Server direct-attached storage (DAS).

### Cache I/O - VERDE Storage Optimization

The Cache I/O refers to two features:

- Write Cache I/O manages copy on write storage.
- Read Cache I/O manages shared storage.

#### EXAMPLE

In an organization with 1000 users all using one shared Windows 7 Gold Image, when all the users try to login to their desktop, 1000 desktops will be connecting to one shared image hosted on the external storage. If each desktop requires at least 50 IOPS (Input/output operations per second) to perform normal operations, then the external storage needs to support at least 50,000 IOPS—and this multiplies with more users in the organization. People also refer to a generic problem known as “boot storm”—when all the users try to boot Windows at the same time when the IOPS are significantly greater than five. To mitigate this problem, more and more drives (spindles) are put in external storage driving up more cost. Some storage vendors also introduce a solid state disk (SSD) based caching blades front-ending the storage. These blades are very expensive.

In addition, there needs to be enough network bandwidth/ports between the VDI servers and external storage server.

The Read Cache I/O storage optimization feature is best used in cluster environments where the Gold Images are stored on shared storage. When enabled, each server keeps a local copy of the Gold Image, avoiding repetitive access to the shared storage when a new desktop starts. The local copy of the Gold Image is automatically updated when changes occur on the shared image.

### Transient Storage Space: Standard Deployment Mode

The Write Cache I/O is used by dynamic desktops to minimize the actual per-user persistent storage of a given Gold Image configuration. For example, if a Gold Image installation consumes 16 GB of storage, each deployed user running a dynamic instance of it might need less than 1 GB of persistent storage space, plus some temporary storage (transient storage) because only the delta from the Gold Image will be stored for each user.

Write Cache I/O requires transient storage. Transient storage requirements vary greatly depending on applications, use, and even runtime length of sessions. However, a conservative estimate is 20% of the Gold Image size for each deployed instance.

#### EXAMPLE

If a template guest installation consumes 16 GB of storage, the transient storage size for each server should be 3.2 GB per user. For 50 concurrent users, assuming the preceding example, it would be 160 GB.

Cache I/O addresses these problems by leveraging the local attached storage (which is less expensive) that is available on each VDI server. Be sure to consider the space needed to store the copies of the Gold Images when sizing the direct attached storage.

### Copy on Write Storage Space for “Long-life” and “Static” Desktops

For sessions that need to persist longer, copy on write storage is on the shared storage device. No Write Cache I/O benefits are available. The storage requirements should be 100%.

After creating a Gold Image, the cache I/O requires synchronization time to complete before images can be launched. Create a group of test users to help gauge the progress of a cache I/O directory synchronization from the User Console.

## Shared Storage Planning

VERDE uses shared storage to store clustering meta-data, provisioning profiles, Gold Images, and user data such as the profile and documents. The size of the required external storage is dependent on:

- **Total user data.**  $U = \text{Number of Users} * \text{Disk space allotted per user}$
- **Total gold images.**  $G = \text{Number of Gold Images} * \text{Gold Image size}$
- **Total meta-data.**  $M = 8 \text{ GB}$

To size the total required external storage, add  $U+G+M$

The performance required from the shared storage depends on the amount of IOPS needed for the user data. Industry guidelines recommend about 5 IOPS for each user profile. The total performance required of the external storage can be calculated as follows:

$P = \text{Number of users} * \text{IOPS per user}$

For a system with 1000 users that each need 2 GB user data space, using 5 Gold Images of 20 GB each, the requirements for storage are as follows:

- **Size.**  $1000 * 2 \text{ GB} + 5 * 20 \text{ GB} + 8 \text{ GB} = 2108 \text{ GB}$
- **Performance.**  $1000 * 5 = 5000 \text{ IOPS}$

## NAS REQUIREMENTS

The requirements for the storage system will depend on the guest sessions to be supported. NFS network file-system supporting:

- NFSv3, and NFSv4.
- NLM file locking.
- POSIX permissions.
- Gigabit or faster networking capacity.
- At least 2.5 Mbps sustained network bandwidth per user.
- Enterprise-class hardware and configuration.

## Sizing Per Desktops

The following tables outline guest session, server, storage, and network requirements needed to determine the server and storage requirements. Use these examples to determine the information needed to implement a physical environment.

Sample Session Requirements

Guest Session Parameters	Sample Requirements
Desktop Type	Dynamic
Total Guest Sessions	800
Concurrent Guest Sessions	800
Virtual CPUs Per Session (vCPU)	1
Memory (GB) Per Session (vRAM)	1.0
Guest Sessions Per Core (core-density)	10
System IOPS Per Session	40
User Profile IOPS Per Session	5

Sample Gold Image Requirements

Guest Image Parameters	Sample Requirements
Number of Gold Images	5
Number of Gold Images Provisioned Per User	5
Average Gold Image Size (GB)	15
Number of Gold Images	5

### Server, Storage, Display Specifications

Server, Storage, Display Specifications	Sample Requirements
Host Total RAM (GB)	192
Host Total Physical CPU Cores	16
Load Factor	80%
VERDE Reserved Host Memory (GB)	8
VERDE Reserved Host Disk (GB)	40
Storage for Applications (GB)	60
Average I/O Block Size (KB)	32
Display Bandwidth Per Session (kbps)	512

These sample requirements would result in an environment with the following components:

- » Servers
  - » 7 servers, with 16c and 192 GB
  - » Storage per server equal to 473 GB
- » External Storage
  - » Shared storage capacity of 1750 GB
  - » Shared storage performance of 4000 IOPS
- » Bandwidth
  - » Shared storage bandwidth of 1000 Mbps
  - » Display bandwidth of 400 Mbps

## Network Planning for Client Access

Several factors related to the infrastructure and the end-user affect the bandwidth use in a VDI deployment:

- » The protocol used for online VDI connections and the specific configuration settings for that protocol.
- » The end-user scenarios that are representative of the real desktop environment.
- » Percentage of users that run on Cloud Branch servers.
- » The number of concurrent users.

### ESTIMATING PROTOCOL NETWORK BANDWIDTH

VERDE server capacity must be planned for peak connected virtual desktop usage. A virtual desktop running on the server with no users connected to it does not typically consume any bandwidth for the VDI session itself. In addition, RDP is primarily an on-demand protocol – when there are no mouse selects, mouse movements, or keyboard activity, no bandwidth is consumed.

It is tempting to measure average bandwidth usage for a single connected user and simply multiply this by the number of peak connected users to estimate the total bandwidth requirement. However, this does not take into account that, at any given instant in time, not all connected users will have activity that directly contributes to bandwidth. There is a real-time nature to bandwidth usage that needs to be taken into account. There may be ten connected users but only two of them are using bandwidth at any given instant in time.

This leads to other anomalies as well. For example, testing with a single user doesn't provide a good indication of the average per-session bandwidth, especially when used for total bandwidth calculations. A single user may have a good user experience at 128 kbps, but 25 users could have the same experience with an average per session bandwidth of 30 kbps. One suggested approach to deal with the situation is to use an effective concurrency when estimating the total bandwidth. For example: **Total Bandwidth (B) = b \* (c/100%) \* n** where

b = per session bandwidth usage      c = concurrency factor      n = number of connected users.

For 150 connected users, 50% concurrency, and 64 kbps per-session bandwidth, this would yield about 4.8 Mb/s of total bandwidth required. Concurrency is a bit difficult to estimate and there is very little data available but 50% seems to be a very conservative number.

A second approach is to effectively account for the concurrency in the per-session number. From industry data, per session value of 30 kbps for RDP has been used for planning purposes. Given this, the same 150 users would yield a total bandwidth of 4.5 Mbps. .  
**Total Bandwidth (B) = b \* n** where

b = average per-session bandwidth usage      n = number of connected users

## NETWORK BANDWIDTH FOR CONNECTED USERS

The per-session remote display and device performance depend heavily on the amount of total network bandwidth available. Generally speaking, the higher the switched bandwidth, the faster and more responsive the end-user sessions will be. In cases where not all users are connected at the same time, the total network bandwidth might be lower without sacrificing session responsiveness, because only a portion of users will be transmitting at any given time.

From the per-user perspective, the following table illustrates the minimum and recommended bandwidth (shown in kbps or Mbps) and latency (shown in milliseconds) figures for various usage profiles.

**Minimum and Recommended Bandwidth**

Virtual Desktop Usage	Spice Access	RDP Access	UXP Access
Casual/Line work	<b>Minimum:</b> 512 kbps/180 ms <b>Recommended:</b> 768 kbps/100 ms	<b>Minimum:</b> 128 kbps/180 ms <b>Recommended:</b> 256 kbps/100 ms	<b>Minimum:</b> 512 kbps/180 ms <b>Recommended:</b> 768 kbps/100 ms
Office/Productivity	<b>Minimum:</b> 768 kbps/100 ms <b>Recommended:</b> 1 Mbps/75 ms	<b>Minimum:</b> 256 kbps/100 ms <b>Recommended:</b> 512 kbps/75 ms	<b>Minimum:</b> 768 kbps/100 ms <b>Recommended:</b> 1 Mbps/75 ms
Multimedia Playback	<b>Minimum:</b> 512 kbps/75 ms <b>Recommended:</b> 1.5 Mbps/50 ms	Not Recommended	<b>Minimum:</b> 512 kbps/75 ms <b>Recommended:</b> 1.5 Mbps/50 ms

Actual bandwidth requirements will vary by exact usage profile, subjective user expectation, and effective network topology. In all cases, the higher the available bandwidth per user, the better the user experience will be. These are per-session bandwidth numbers only. When estimating total bandwidth for a large number of users, a concurrency factor should be used along with this per-session value, as indicated above. Several protocol-specific parameters have a significant effect on bandwidth. For RDP, the significant parameters are:

End-user scenarios need to be representative of real-world workloads. Ultimately, setting up a pilot environment with real users and measuring bandwidth usage is the most accurate way to estimate the overall bandwidth requirement.

## Guest Image RAM and Disk Space Planning

Multiple guest sessions can be accessed from a client and run on the VERDE Server. Knowing the different types of sessions will help determine the VERDE Server requirements.

### SUPPORTED GUEST VIRTUAL DESKTOP SESSIONS

The guest or virtual desktop itself is also called the VDI session. SPICE is the remote-display system used to edit Gold Images and is available for all supported guest sessions.

When creating a guest image, the following can be defined:

- On the **Session Settings** screen, set the number of GB for the user files virtual disk image (in Windows, the D: volume, in Linux, the /home directory).
- On the **Gold Images** screen, set the amount of virtual RAM used by the guest image and the # of GB used by the operating system virtual disk image (in Windows, the C: volume; in Linux, /).
- The amount of virtual RAM used by the guest image and the # of GB used by the operating system virtual disk image (in Windows, the C: volume; in Linux, /).
- **For Windows VDI sessions:** The user's profile settings are stored on volume D: and user documents are stored on the shared folder by default. This does not count toward the 2 GB allocated space.

## Supported Platforms

The host server is where the VDI guest sessions (also referred to as virtual desktops) will run. The server and client machines must meet the requirements as described below.

- **Intel** \*<sup>®</sup> Virtualization Technology (VT)& Intel x86 processor, or **AMD-V**<sup>™</sup> capabilities & AMD x86 processor
- Server-class CPU (Intel Xeon 55xx or newer recommended for best performance)
- 8 GB of RAM for the system + RAM to run virtual desktops
- 15K RPM SAS disk with a capacity of 100 GB or more (contingent on # of Gold Images and users)
- Wired network, 1 Gbps Ethernet

### Software

The following operating systems are supported with latest updates and service packs:

- Ubuntu 14.04, 16.04
- Red Hat Enterprise Linux (RHEL) 6.9/7.x
- Community Enterprise Operating System (CentOS) 6.9/7.x



## SUPPORTED GUEST SESSIONS

The following tables list the supported virtual desktops or guest sessions, and their supported protocol.

Windows Guest Sessions

Windows Operating System	SPICE	RDP	UXP
Windows Server 2008, 32-bit	✗	✓	✗
Windows Server 2008 R2 Datacenter Edition 64-bit Support	✓	✓	✓
Windows Server 2012 R2, 64-bit Support	✓	✓	✓
Windows 7 (including SP1) 32-bit Support	✓	✓	✗
Windows 7 (including SP1) 64-bit Support	✓	✓	✓
Windows 8.1 32-bit Support	✓ *	✓	✗
Windows 8.1 64-bit Support	✓ *	✓	✓
Windows 10 32-bit Support	✓	✓	✗
Windows 10 64-bit Support	✓	✓	✓
Windows 2016 32-bit Support	✓	✓	✗
Windows 2016 64-bit Support	✓	✓	✓

\* Limited functionality - No QXL driver available for Windows 8.1

#### Linux Guest Sessions

Linux Operating System	SPICE	Accelerated SPICE Access	RDP Access
CentOS/RHEL 6.x32-bit Support	✗	✓	✗
CentOS/RHEL 6.x 64-bit Support	✗	✓	✗
Ubuntu Desktop 12.04 32-bit Support	✗	✓	✗
Ubuntu Desktop 12.04 64-bit Support	✗	✓	✗
Ubuntu 1404	✗	✓	✗
Ubuntu 1604	✗	✓	✗
LinuxMint	✗	✓	✗
CentOS 7	✗	✓	✗

## Multiple Methods of Installation

### VERDE INSTALLED ON BARE METAL SERVER (VERDEOS)

Installing VERDE on bare metal takes advantage of a pre-built VERDEOS ISO file that will, when installed into a bootable DVD drive or bootable USB Stick, begin by reformatting the destination drive of the server and installing a pre-defined VERDE built distribution of CentOS 7.x followed by the installation of the VERDE VDI 8.2.7 binaries. Once installed, VERDE will present a configuration menu to the system administrator to provide site specific details regarding network address, NAS storage setup, and Cloud Branch locations.

There are limitations to the use of the VERDEOS method. As vendor hardware may have variations in what is provided by different vendors, not all needed drivers can be guaranteed to have been built into the predefined CentOS image created by VERDE at the time of release. In this case it is recommended that the non-bare metal installation option be chosen.

### VERDE INSTALLED ON NON-BARE METAL SERVER (RPM METHOD)

Installing VERDE on non-bare metal assumes that a server has been pre-configured with a CentOS or Red Hat 7.x ISO and VERDE specific configuration options have been applied. Once, the server is properly pre-configured with the OS, the VERDE application RPMs can then manually be applied. Once VERDE is installed a command line configuration script is invoked to obtain the necessary site-specific information. The limitation here is that while the RPM method allows for the most current hardware support and drivers from Red Hat are available, a qualified Linux systems administrator is highly recommended to perform this type of installation.

## Common Installment Requirements

Installing using the VERDEOS method or the RPM method have the same requirements for the majority of use cases for VERDE VDI Hosting. Difference, if any, will be described in the relevant Installation steps outlined in later sections of this document.

### VERDEHOSTING

VERDE VDI can be installed either on premise or in a hosted cloud environment both virtually and a dedicated physical server. We currently host our own VERDE installation in the IBM Cloud provisioning on physical servers and Microsoft AZURE which provisions virtual servers.

In some installations of VERDE, it may be advantageous to also run a VERDE Cloud Branch installation in a remote office. This provides for high speed LAN-based virtual desktop access when a WAN connection from the remote location is not a viable option. In these cases, the same rules apply to the use of bare metal servers for the designated VDI servers.

The elements of VERDE that can be run in a virtual server are:

- Network attached storage required for managing in a VERDE cluster.
- The VERDE Cluster master and potentially the VERDE Cluster Master failover candidates used for high availability.
- The VERDE Gateway for workload and IP distribution.
- Optionally, any LDAP server used for account authorization and roaming user profiles.
- Optionally, any Third-Party Backup and recovery application management software used for business continuity.

## Clustering Requirements

VERDE VDI can consist of a single server installation or can run in a cluster of VERDE servers. There is no predefined limit as to the number of servers that can be supported in a single cluster but shared network band width and shared storage limitations need to be accounted for when evaluating your end user desktop needs.

Once a single server is configured to use shared storage (NAS, SAN or CIFS), adding additional servers to build a cluster consists of installing VERDE VDI on a new server and configuring the type of services this server will provide. If the server is to be used as a failover Cluster Master it must, at a minimum, be designated as a Cluster Master server.

In a clustered environment, all VERDE servers must be running the same version of VERDE and all servers must be time-synced to the same NTP service.

All the servers in a cluster must be installed using the same method of installation, either using VERDEOS or RPM based installation. This is also true regarding a Branch server. If a Branch is added, it needs to be the same install method as the CM.

## UPGRADING VERDE REQUIREMENTS

When upgrading VERDE to a new version, it is important to keep in mind that upgrades must also be continued to be either VERDEOS or RPM based depending on the original fresh install of VERDE VDI. You can however use rpms to upgrade VERDEOS. But, you cannot use VERDEOS to upgrade rpms'.

## Installing VERDEOS

Installing VERDEOS begins by downloading the VERDEOS ISO file. A link to the ISO is provided to you in the NComputing Management Portal when you requested a trial version or when you purchased VERDE VDI. When first installing a trial copy of VERDE VDI, you will be supplied with a temporary trial user license key that you will need to redeem using the VERDE Management Console as the final step in the installation process.

### INSTALLATION STEPS

#### INSTALLATION PREREQUISITES

- The VERDE for bare metal installation (VERDEOS) is a self-installing software package. Burn the installation package .ISO file to a bootable DVD or USB stick. Keep the following in mind.
- When using external storage in a cluster environment, the external storage must be connected and accessible from the servers prior to installing. Please refer to the Administrator Guide for more details.
- Confirm the machine contains the number of network interfaces necessary to support VERDE guest and management traffic. These interfaces will be configured through the VERDE Menu as a step in the installation process
- All machines in the VERDE environment must be installed with the same installation type—VERDEOS or RPM based — including the data center cluster and any Branch Servers.

To facilitate the installation, collect the data listed in the table below prior to starting the installation.

- Static or dynamic IP address for the server.
- Subnet or netmask address.
- Broadcast IP address.
- Default Gateway IP address.
- Primary/Secondary/Additional DNS Server Address(es).
- Public IP Address or FQDN of the server – The hostname or IP address for clients to connect to this server.

## Installing the VERDEOS Package

Boot the host server from the VERDE bare metal installation CD or USB device containing the installation package. A **VERDE VDI Welcome** screen will be displayed. Select one of the following options:

- Boot from local drive (skip the installation of VERDEOS from the bootable DVD or thumb drive)
- Quick Install\*. Automatically partitions and formats ALL attached storage devices
- Expert Install. (Manually partition and format storage devices.)
- Upgrade an existing system to this version of VERDE.

**Note:** You may only upgrade VERDE from the most current previous version of VERDE. THERE IS NO UPGRADE PATH FROM A CENTOS6.x based VERDEOS to CENTOS7.x VERDEOS.

\* It is recommended that you select the quick install method unless you require specific Linux disk partitioning settings.

### QUICK INSTALL

Select the "Quick Install" option from the main menu of the **Welcome** screen. This option automatically partitions the server drives.

1. On the **Choose Language** screen, select a default language, then select "Next."
2. On the **Time Zone** screen, choose the time zone for the server and determine if UTC (Coordinated Universal Time) is used. After picking a time zone, select "Next" to prompt the installation to begin.

**Note:** The process of formatting and partitioning storage takes several minutes. When this step is completed, you will see the Installing VERDE progress bar. When the installation completes, the system will automatically reboot.

3. Enter a user administration password after installation is complete.
4. Enter a root password for the root user and confirm it.
5. After the **Welcome** screen appears, press "F6" to open the VERDE Menu to the **Network Configuration** screen.

**Note:** Take note of the '\*' in the welcome message and in the menus to follow; the '\*' denotes items that require configuration in order to start the system and VERDE services

## NAVIGATING THE VERDE MENU

The VERDE Menu enables networking, server, and storage configuration. The following procedures provide a general workflow for installing and configuring the system:

- Menu items with an asterisk (\*) are required to start VERDE Services.
- Press "F5" to back to a previous step.
- Press "F6" to go forward to the next step in a sequence.
- Menus that have sub-menus are marked.



The VERDE Menu consists of the following options.

- |  |                                   |
|--|-----------------------------------|
| >> Network Configuration               | >> Branch Configuration           |
| >> Stop System Services                | >> Restart the Management Console |
| >> Generate Support Report             | >> Power Off this Server          |
| >> Server Configuration                | >> Start System Services          |
| >> Stop System Services and Networking | >> Root Shell                     |
| >> Reboot the Server                   | >> Log out of Menu                |



## ACCESSING THE VERDE MENU REMOTELY

After the initial setup, the VERDE Menu can run remotely through an SSH connection as admin or root. Networking must be configured and started on the VERDE server to access the VERDE Menu remotely. If logging in via SSH with the admin credentials you will be taken directly to the menu.

**Note:** If logging via SSH as 'root', you will need to enter `/usr/lib/verde/bin/verde-menu` from the command line in order to access the menu.

### Network Connection

The network configuration portion of the menu can be accessed during or after installation to configure VLAN tagging and bonded pairs. When configuring OpenvSwitch on the server, the networking configuration program performs the following tasks:

- The program discovers each free interface and asks to configure it.
- The program tests the network for confirmation that the configuration is valid.

When Session Settings are created in the VERDE Management Console, assign the network name and any VLAN tags to enable guest sessions to access these settings.

1. From the **Main Menu**, choose the "Network Configuration" option.
2. Press "Enter," then select the **Network Configuration Wizard**.
3. Press "Enter." The **Choose Interface** screen will be displayed. VERDE detects the available network interfaces and lists them incrementally. Configure the interfaces that VERDE will be using. Enter the option number to configure an interface:
  - **vbinat0: NAT interface.** This is pre-configured for VERDE system use; keep the default unless the "192.168.84" network is already in use.
  - **em1 interface.** This is the first network interface detected.
  - **em2 interface.** This is the second network interface detected.
  - **Use Standard Network Configuration.** This option enables VERDE to use standard Linux networking.

**Note:** Additional interfaces will be listed if they are detected.

4. Press "Enter." The NIC Usage screen will display.
5. Select the "Form new Network" option. If this is not the first interface to be configured, other options will be displayed.
6. Press "Enter." Type a name for this interface in the "Enter a name for the Network" field or keep the default
7. Press "Enter." In the "Enter the MTU for this Network" field, define the maximum size for a package as it travels across this network. The default is 1500.

**Note:** When configuring VLAN, it is recommended to use at least 1504

8. Press "Enter" to continue. The **Network Host-Access/VLAN Configuration** screen will be displayed.

The following options are available:

- Add VLAN or non-VLAN Host-Access
- Configure non-VLAN Host-Access (present after initial configuration)
- Remove non-VLAN Host-Access (present after initial configuration)
- Go back to previous step (F5)
- Continue to next step (F6)

9. Select the "Add VLAN or non-VLAN Host-Access" option to define the first network interface.

10. Press "Enter." Type a VLAN Tag for this network. A value of "0" defines non-VLAN trunk port. If configuring only one network, enter a value of "0."

11. Press "Enter." Define if the VLAN will obtain the network address from DHCP (Y/N).

If no, you'll need to configure the following options:

- a. Will this interface provide the server's public address? (Y/N) This is the address used to connect to the VERDE Server. Press "Enter."
- b. Enter the Host Access IP Address. Type an address and press "Enter."
- c. Enter the Host Access Netmask. Type the netmask and press "Enter."
- d. Enter the Host Access Broadcast Address. Type the address and press "Enter."

If yes for DHCP, only the prompt for the server's public address will display. Choose (Y/N) and press "Enter."

12. The menu returns to the **Network Host-Access/VLAN Configuration** screen.

Multiple VLANs can be added from this screen:

13. Select an option to add or configure another interface, change a setting that was just configured, or press "F6" to continue to the next step. "F6" will display the **Choose Interface** screen. If DHCP is not configured for any of the network interfaces, the **Default Route/Gateway Setup** screen will display. Based on previous options, a default route may be entered. Press "Enter" to accept the default or type a new address.

14. On the **DNS Server Setup** screen, enter the DNS Server address for the network, then press "Enter." Separate multiple entries with commas.

15. After interfaces are configured, the **Server Roles** screen will be displayed.

## SERVER AND STORAGE CONFIGURATION

1. On the **Server Configuration** screen, choose menu item 2 and press "Enter."
2. On the **Server Role** screen, choose one of the following roles for the sever:
  1. Cluster Master + Management Console + VDI Server (default)
  2. Cluster Master + Management Console (does not host VDI sessions)
  3. VDI Server only (cluster node)
  4. Gateway only (connection broker)
3. Press "Enter." On the **Public-Address** screen, enter the IP address or externally available host name that external clients will use to connect to this server.
4. If you are using external storage (required if setting up a clustered VERDE environment), on the **External Storage Type** screen, select one of the following options:
  1. CIFS-style mount (Windows)
  2. NFS-style mount (Linux Server)
  3. Do not configure mount-point
5. Press "Enter."
6. If you choose either option 1 or 2, provide additional External Storage mount information, including the NFS or CIFS server IP address and NFS or CIFS mount path.
7. Press "Enter."
8. Enter "6" to exit to the Main Menu.
9. Select "Network Configuration."
10. Select option 5, "Test Network."
11. Select option 7 "Return to..."
12. On the **Network Configuration** sub-menu, select "Restart Network." If the networking settings are valid, a success message will display.

## Installing VERDE Using RPMs

Installation using the RPM method is recommended when there is a specific IT mandate for a company approved CentOS or Red Hat corporate standard. In these cases, installing a pre-configured VERDEOS is not your best solution. A second reason for using the RPM based installation method is valid for customers who want more fine-grained control over the settings and packages installed in their Linux operating system. Finally, while VERDEOS is good for many installations, when new hardware or updated driver packages are released for a Linux distribution, it is not always possible or practical for VERDEOS to stay current on these updates. In these cases, VERDEOS may not be suitable for the newest hardware, and the RPM installation method will more than likely support those latest updates.

If using the RPM method, it is assumed that you have already downloaded and installed Red Hat or CentOS on your server. You will also need to obtain a set of VERDE RPMs from NComputing. Contact your NComputing sales partner to acquire about these packages.

### CONSIDERATIONS

- It is assumed that an intermediate level of Linux administration skills exists and that there is a network in place on the server that will allow access to an external site for installing updates and VERDE licenses.
- While RDE 8.x will run on any CentOS or Red Hat version from 6.4 through 7.x, our engineering and QA reference model was based on CentOS 7.x. As well, there's no upgrade path from Centos6.x to Centos 7.x. So, please go with Centos7.x..
- All servers in a cluster must be installed with the same installation type, in this case using the RPM installation method. Each server in a VERDE cluster requires the same RPM version and VERDE-specific base configuration settings.
- Tomcat installs as part of the VERDE installation package; therefore, it is unnecessary to install virtualization support or Tomcat during the operating system installation.
- Register with Red Hat Network (RHN) to install additional packages using yum.

## Configuring VERDE using the RPM Method

### ENABLE VIRTUALIZATION

Confirm that virtualization (VT) is enabled in the BIOS.

To verify that the CPU is virtualization capable, run the following commands:

#### **Intel processors:**

```
egrep '^flags.*(vmx)' /proc/cpuinfo
```

#### **AMD processors:**

```
egrep '^flags.*(svm)' /proc/cpuinfo
```

If neither command produces an output, then virtualization is not enabled. Boot into the server bios and follow the hardware vendor's steps to enable VT support.

### MOUNTING SHARED STORAGE (REQUIRED FOR CLUSTERED VERDE ENVIRONMENTS)

Shared storage is an important consideration when installing VERDE. Shared storage is a requirement for any VERDE clustered implementation, but it can also be valuable when starting out with a single server. VERDE maintains its internal structures in `/home/vb-verde`, and therefore needs access to this folder— whether in a single server or clustered environment. By starting out on a single server with an attached network storage device, future upgrades to a multi-server VERDE installation will be much easier, as you will not have to move `/home/vb-verde` to a NAS device later when two or more servers need to share the single instance of a common vb-verde structure.

When installing VERDE with a NAS device, CentOS requires a custom partition layout to keep `/home/vb-verde` from being created as a local file path during the VERDE installation.

## PRE-INSTALLATION CONFIGURATION STEPS FOR VERDE

Prior to installing the VERDE RPMs, a number of basic CentOS configuration steps need to be performed:

- Ensure the server network connection is enabled and that you can ping the gateway from the server
- Ensure you can ping the server from the workstation/client you're going to use to access the VERDE User Console and VERDE SW Client
- As root, run the following updates. Note: that some may have already been installed via the previous yum updates and these commands should be run as verification.

```
yum -y update
yum -y install epel-release
yum -y --enablerepo=updates --enablerepo=base --assumeyes update openssl
yum -y --enablerepo=updates --enablerepo=base --assumeyes install java-1.8.0-openjdk.x86_64
yum -y --enablerepo=updates --enablerepo=base --assumeyes update libpng
yum -y install gtk2
yum -y install zip unzip
yum -y install bridge-utils
yum -y install net-tools
yum -y install genisoimage
yum -y install libogg
yum -y install libvorbis
```

- If you are planning to use a NFS/NAS (Shared Storage Device), perform the following before installing the VERDE software:

- Run the following on the local server (not the NAS/NFS)

```
# yum -y install nfs-utils nfs-utils-lib
```

- Run the mount command. It must include the mount command, the data format, the desired flags, the server name, storage volume and where it's being mounted to .... /home/vb-verde.

Here are two examples:

```
# mount -t nfs4 -o rw,noatime fsf-dal1001b-fz.ad-
n.networklayer.com:/SL02SEV1317203_1/data01 /home/vb-verde
# mount -t nfs -o rw,noatime 10.10.1.104:/nfs/VerdeNAS /home/vb-
verde
```

The mount command must be included in the /etc/fstab file. Here's an example:

```
192.168.0.15:/volume1/vbshare /home/vb-verde nfs4 rw,noatime 0 0
```

- Create the vb-verde user with a password that never expires.

```
# useradd vb-verde
```

```
# passwd vb-verde
```

- Then add vb-verde to the root group:  
# usermod -G root vb-verde

Confirm that the following items are true for this account:

- The account is not the root user.
- The password of this account will not expire.
- The UID/GID must be identical across all servers.
- The account has a unique home directory that resides on the same file system as the VERDE Server.

Create the following file: (include the \*– in the text on each line)

```
#vi /etc/security/limits.d/95-verde.conf
```

```
*- nproc - 1
```

```
*- nofile 65535
```

Set JAVA 8 as the default java version:

```
# sudo update-alternatives --config java
```

VERDE is inherently secure with its use of TLS security and encryption however you will need to ensure that specific ports are available for certain tasks.

#### Ports and Their Functions

Port	Used for
8443	Access to the Management Console
48622	Access to Spice connection
48632	Optional for customers using cloud branch (Smartsync) technology
22	Optional for times when the admin wants to SSH into the VERDE server

During the installation, we suggest you simply disable security to save time. (For security reasons, we recommend that the use of iptables or some other firewall mechanism be in place prior to production.)

Disable (permanently) iptables using the following 2 commands:

```
# systemctl stop firewalld  
# systemctl disable firewalld
```

SELINUX: (at a minimum, SELINUX must be in permissive mode—normally we suggest disabling it)

```
#vi /etc/sysconfig/selinux  
SELINUX=disabled
```

## Installing the VERDE RPMs

Copy all VERDE RPM's to the server's root directory. They should resemble the following (dependent on the build number):

- VERDE-<rel>-<build>-x86\_64.rpm
- VERDE-clients-rel-.x86\_64.rpm
- VERDE-core-rel-.x86\_64.rpm VERDE-guests-rel-.x86\_64.rpm
- VERDE-network-rel-.x86\_64.rpm
- VERDE-web-rel-.x86\_64.rpm
- VERDE-rel-.x86\_64.rpm

Run the following install command:

```
# yum --nogpgcheck install *.rpm
```

You will be asked several questions. Reply "yes" to all of them.



## CONFIGURING THE VERDE ENVIRONMENT

In an RPM-based installation method the configuration script can run in interactive, menu, or in unattended modes.

- Run the script as root with the following command:  
# /usr/lib/verde/bin/verde-config -i
- Once the configuration applet completes the VERDE service will automatically be stopped:  
# reboot
- When VERDE comes back up, ensure the service is running:  
# service LICSRV status

Verde-config Script Options

Script Options	
-h	Prints command help.
-u	Starts an unattended configuration, which requires an answer file.
-m	Starts a menu-based configuration, which enables direct access to specific parameters.
<none>	If VERDE has already been configured on this server, this option sets up some system files and restarts VERDE. Otherwise, an unattended installation is performed (with optional parameters provided with VERDE_CONFIG_CMDLINE).
-i	Starts an interview-based (interactive) configuration with prompts to answer all configuration questions. If a default value is available, it is listed. Press Enter to accept the default value. If no value is present, pressing Enter will leave the value empty.
-f <file>	Specifies an answer file to be used with an unattended installation.
-l	Specifies that only the local server configuration is updated (/var/lib/verde/settings.node).
-n	Specifies no restart of the VERDE Server when finished.

Using the `-i` command line option walks you through the standard configuration options needed to properly configure VERDE. All of the configuration questions will have a default value and for the most part these default values will be sufficient. You will not have defaults for the required network IP information, and you will need to be prepared to have the IP address for your internal and external network IPs, your gateway, and DNS server.

To launch the interactive configuration script use:

```
# /usr/lib/verde/bin/verde-config -i
```

## CONFIGURATION SCRIPT QUESTIONS

Run the VERDE script with the following command to view all questions:

```
# /usr/lib/verde/bin/verde-config -i
```

Once completed, a configuration summary is displayed. Press "ENTER" to save changes. VERDE will restart or press "Ctrl+C" to quit without saving changes.

Configuration Script

Interactive Mode Questions	Description	Default Value
What is the VERDE Management Console account?	This account owns the VERDE configuration files, Gold Images, and related configuration settings. The VERDE software runs with the privileges of this account as a system account. When entering names that contain backslashes, be sure to enter a corresponding escape sequence by typing two backslashes. For example: domain\\vb-verde If the letter that follows the backslash is "n", "r", or "t" then enter four backslashes. For example: domain\\\\\\nt\\user	vb-verde
What is the role of this server?	Option 1) The server can act as a cluster master, runs the VERDE Management Console, but will not host VDI sessions. This option is typically used in clustering environments. Option 2) This server is a cluster master candidate, runs the VERDE Management Console, and hosts VDI sessions. Select this option for standalone server deployment or in cluster configurations for cluster master fail-over. Option 3) The server only hosts VDI sessions. This option is used in cluster environments with multiple servers. Option 4) A gateway server relays VDI connections to other servers shielding them from direct internet connections. It does not host VDI sessions nor serve as a cluster master candidate.	2
What is the public IP or FQDN of this server, to be used for management traffic?	Enter the public IP or the fully qualified domain name of this server. This name or address needs to be resolvable from other servers in the cluster. Note: VERDE Management Console uses this information for reporting. If the IP address is used instead of the server name, changing the IP address requires editing this value in the verde-config script.	<Servername>
What is the public IP or FQDN, to be used for user traffic?	This is the address for VERDE User Console connections. The default is the address entered in question 3.	<Servername>

What are the initial resource tags for this server?	<p>Categories are pre-defined and not editable:</p> <ul style="list-style-type: none"> <li>&gt;&gt; ORG: tags for organizations. The format is ORG:orgname-&lt;org id&gt;. Web names can also be used as tags.</li> <li>&gt;&gt; NETWORK: network tags. The format is NETWORK:network_tag.</li> <li>&gt;&gt; HARDWARE: tags determined by VERDE about server hardware and not editable.</li> <li>&gt;&gt; OTHER: user defined tags, including computer resource tags. To create a tag, such as a resource tag enter OTHERresourceTag1.</li> </ul> <p>The list of tags within a category will also support a wildcard option (*). When ORG:* is specified, it is a shortcut for specifying a list of all available organization tags. VERDE event reports all known tags using the same value format.</p>	No default and can be left empty.
How often should branches synchronize?	This parameter defines how often the changes to the Gold Images, settings, deployment rules, and related settings will be synchronized with the central server.	5
Is this a branch server?	If this is a VERDE Cloud Branch environment, one branch download server is required per branch. Select "Yes" if the server is a cloud branch server. Additional questions display.	No
On which port should VERDE Management Console and VERDE User Console run?	Enter the https port on which the User Console is available to end users. The VERDE Management Console and User Console will also communicate on port 8080.	8443
What character should be used to replace space characters in user names?	In order to be able to use spaces in user names, the space must be substituted by a "dummy" character. This character will be used by PowerBroker during the authentication process with Microsoft Active Directory. For example, the "User Principal Name" or "UPN" would be "test^user" where the space is replaced the "^" symbol.	^


The following settings are used only when Read Cache I/O is enabled in the VERDE Management Console

These settings apply to cluster environments where multiple servers share a central storage (NAS).

## CONFIGURING THE BRANCH SERVER

### Configuring the Branch Server

Interactive Mode Questions	Description	Default Value
How often should VDI nodes synchronize gold images from external storage (1-600 minutes)?	If a Gold Image update is available, it will be synchronized with the cached copy of this Gold Image stored on the local node. This parameter defines the synchronization frequency. The default is 1 minute. Unlike the rest of the values in this table, this is configured in the data center, where branch servers connect.	1
What local directory should be used for Write Cache I/O (leave empty to use users' home directories)?	The directory where temporary changes (transient storage) to the system volume (such as the C: drive) will be stored. Confirm there is enough space. Those changes will be lost at initialization of the next session. If left blank, the user's home directories will be used. Use "^D" to denote an empty string. If another value is used, such as /tmp, that directory must be writable by all. To make the directory writable, change the permissions (777). To improve performance in a cluster environment, directly attach a drive for this folder.	
What is the address of the SmartSync server?	Enter the address (IP or FQDN address) of the server in the data center that is going to handle the data synchronization (Gold Images, configuration files) with the branch. This can be a single server address as well as a FQDN that will provide a round robin DNS resolution to a node in the cluster. The Branch Server requires credentials for downloading updates from the SmartSync server. Enter the credentials for this operation. Backslashes are not supported in passwords and passwords will not be echoed back to the terminal.	None
Enter the Active Directory domain for logging in to the Smart Sync server.	This step is only required if your SmartSync user is an Active Directory user. If it is, enter the AD domain for logging in to the Smart Sync server. For example, ADNETWORK	None

Enter username for logging in to the SmartSync server.	<p>The Gold Image synchronization process authenticates with this user on the cloud server in the data center.</p> <p>The username and password specified for Branch synchronization be a Master Console Administrator in global space.</p>	None
Enter password for logging in to the SmartSync server.	Enter and verify the password of the user defined in the previous question.	None
How often should branches synchronize (1-1440 minutes)?	This parameter defines how often the changes to the Gold Images, settings, deployment rules, and related settings will be synchronized with the central server.	5
Enter time of day at which user data will be synchronized (00:00 - 23:59)?	<p>This parameter defines the time of day when the user data (from My Documents in Windows, for example) will be backed up on the cloud server in the data center, for example at 05:45. Enter "NEVER" to disable user data synchronization.</p> <div>  <p><b>Note:</b> This can happen only once a day and user documents must be stored outside of the user image for the synchronization to work properly.</p> </div>	None

## RUNNING THE CONFIGURATION SCRIPT IN MENU MODE

The VERDE configuration script can also run in menu mode, which enables direct access to specific parameters. Run the script with the following command:

```
# /usr/lib/verde/bin/verde-config -m
```

These options are listed as:

```
*** VERDE Server Configuration ***Please select an item to configure:

1) Set VERDE Management account

Node settings:

2) Set server's role
3) Set role-specific settings

Cluster settings:

4) Set VERDE Administrator user account
5) Set VERDE Branch download settings
6) Set other cluster-wide settings
7) Set Read Cache/O settings
8) Set Write Cache/O settings

General:

v) View configuration
s) Save settings, restart VERDE and exit
q) Quit without saving
```

Select an item and press "Enter." A subset of interview questions is listed.



## RUNNING THE CONFIGURATION SCRIPT IN UNATTENDED MODE

The VERDE configuration script can run in unattended mode. This enables quick set up of several servers, which is useful when VERDE is deployed in a cluster environment. Cluster-wide settings only need to be configured once. It is possible to run concurrent installations on multiple servers.

The setup parameters are defined in a configuration file that is specified as an option when running the script. Run the script with the following command:

```
# /usr/lib/verde/bin/verde-config -f <file> -u
```

A sample answer file is provided in `/usr/lib/verde/etc/verde-config-answer-file.txt` as a template. The file can be located anywhere on the server. Specify the correct path when running the configuration script.

The `verde-config-answer-file.txt` contains the following. Update it according to your requirements.

```
# Sample verde-config answer file

# ----- VERDE Node configuration -----

#

# mc_user default: vb-verde
# server_role values: CM_Only, CM_VDI, VDI_Only, Gateway; default: CM_VDI
# pubaddr required only if server_role is CM_VDI or VDI_Only; default: out-
put # of hostname -f
# debug_level values: note, info, dbg; default: note
#

#mc_user="vb-verde"
#server_role="CM_Only"
#pubaddr="192.168.1.100"

# ----- VERDE Cluster configuration -----

#

# master_admin default: mcadmin1
# leaf_update_port default: 8080
# username_space_replacement default: ^
```

```
#master_admin="mcadmin1"
#tomcat_port="8443"
#leaf_update_port="8080"
#username_space_replacement="^"
#
# ----- Cache I/O configuration -----
#
# snap_dir default: empty
# cacheio_dir required if cache I/O will be used, default:
# /var/lib/verde/cacheio
# cacheio_sync_interval default: 4 minutes
#
#snap_dir=""
#cacheio_dir="/var/lib/verde/cacheio"
#cacheio_sync_interval="4"
#
# ----- Branch server configuration -----
#
# cloud_addr if empty then server is not a branch server
# cloud_username required if cloud_addr is not empty
# cloud_password required if cloud_addr is not empty
# cloud_domain default: empty
# branch_user_data_sync_time default: 1:00 (i.e. 1 AM)
# branch_sync_interval default: 5 minutes
```

```
#  
#cloud_addr="10.0.7.100"  
#cloud_domain="DOMAIN"  
#cloud_username="admin"  
#cloud_password="123456"  
#branch_user_data_sync_time="02:00"  
#branch_sync_interval="5"
```

There are two methods for beginning an install on a multi-server environment:

- Install the first node manually, then use it to build and test the response file.
- Use the unattended method to install all of the nodes.

Since the cluster will likely include a mix of cluster master candidates as well as VDI-only servers, two response files are needed:

- Cluster master candidate response file
- VDI server response file

### Cluster Master Candidate response file (example answer.cm)

Update as many parameters as needed. However, the server role must be set to "CM\_VDI"

```
# answer.cm
```

```
server_role="CM_VDI"
```

### VDI Server response file (example answer.vdi)

Set the server role to "VDI-Only"

```
# answer.vdi
```

```
server_role="VDI_Only"
```

## RUNNING THE UNATTENDED INSTALLATION

It is possible to use environment variables to run the VERDE installation. Command line options can be entered with the VERDE\_CONFIG\_CMDLINE variable.

**Note:** To upgrade the VERDE system, on rpm-based distributions (CentOS/RHEL), remove the VERDE package prior to running the installation command.

First confirm the VERDE installation package is available to all the nodes, then install.

### **RPM-based installation:**

```
VERDE_CONFIG_CMDLINE="-f <response file> -u" rpm --install <VERDE package>
```

### **On the Cluster Master Candidate Nodes**

```
VERDE_CONFIG_CMDLINE="-f /home/vb-verde/temp/answer.cm -u" \ rpm --install VERDE-7.0.xxxxx.x86_64.rpm
```

### **On the VDI Nodes**

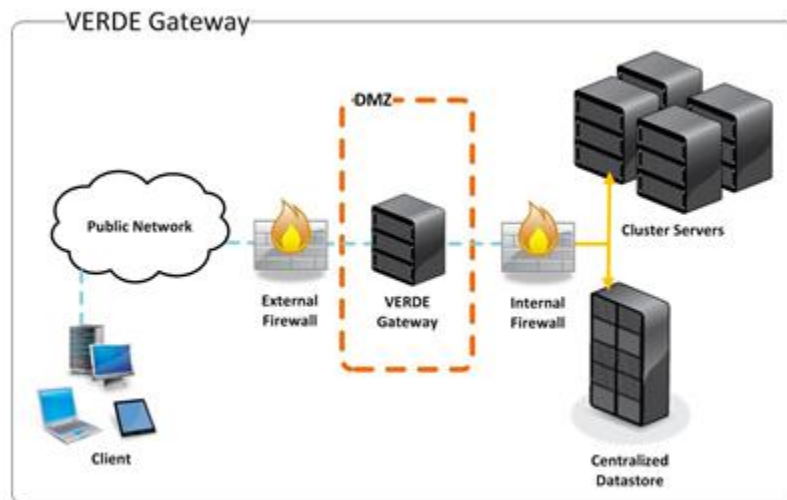
```
VERDE_CONFIG_CMDLINE="-f /home/vb-verde/temp/answer.vdi -u" \
```

## Configuring Isolated Gateway Servers

### VERDE GATEWAYS

A gateway is a server network node that provides access into and out of a network. Set up VERDE Gateways to communicate with VERDE servers located in a secure environment. VERDE Gateways reside within the Demilitarized Zone (DMZ) to reduce exposure to internal servers. VERDE Gateways provide secure public network access and grant remote users proper access to the internal network where VERDE, applications, resources, and internal data resides. Communication between client devices and the isolated gateway is encrypted. Users must log in to the secure network with valid user credentials to access their virtual desktop (s).

This figure shows one of many ways to set up this configuration.



### REQUIREMENTS FOR A GATEWAY ENVIRONMENT

An isolated gateway requires the following:

- At least one VERDE server.
- At least one network interface controller (NIC) with access to both internal and public networks, or two NICs (one for internal access and one for external).
- Configure Isolated Gateway Servers to reside within the authorized demilitarized zone (DMZ).

## PREPARATION FOR A GATEWAY ENVIRONMENT

Before configuring the cluster master and the VERDE Gateway servers, prepare the following:

- Download the VERDE installation package onto the cluster master candidates and the Isolated Gateway server(s).
- On the GTW server, designate a system user (vb-verde) with the same UUID and GUID as the infra structure. The system user is the designated isolated gateway administrator role.
- Determine the IP addresses of each cluster master candidate. Set up of Isolated Gateways requires a list of assigned server IP addresses for use during VERDE configuration.
- Set up the following ports to facilitate communication between the public network and the internal data center via the Isolated Gateway host(s).
- Public Network —> DMZ

48622 Public IP —> 48622 Gateway IP

443 Public IP —> 8443 Gateway IP (or forward 8443 —> 8443. The first setting does not require appending a port on a URL).

- DMZ —> Internal Network

Secure LDAP —> port 636 (encrypted) or 389 (non-encrypted) on the LDAP server Clear LDAP —> port 389 on the LDAP server 48616

Gateway IP —> 48616 cluster master IP(s) 48622 Gateway IP —> 48622 VDI server IP(s)

Virtualization on the server is not required because the Isolated Gateway is not used to host VDI sessions. Isolated Gateway(s) acts as a proxy for the cluster master, and UXP, SPICE or RDP traffic.

Only configure the vb-verde user with matching UID/GID on CM/VDI satellites (RPM based installation methods).

**Note:** Configure the VERDE gateway in a test environment prior to implementing it in a production environment to ensure that all settings work correctly

## GATEWAY CONFIGURATION SETTINGS

### Gateway Configuration Settings

What is the VERDE Management Console account?	Enter the vb-verde user or the equivalent VERDE Console system account user defined on the VERDE Server for the designated environment.
What is the role of this server?	Enter option 4: VERDE Gateway only (connection broker).
Is this an Isolated Gateway server?	Enter yes.
What is/are the public IP address(es) or FQDN('s) of the Cluster Master(s)?	The public IP address or FQDN is not needed on a Gateway server. When specifying multiple addresses, separate them by semi-colons. Enter a semicolon delimited list of the IP address(es) of the cluster master candidate(s) in your environment (for example, CM_Only or CM_VDI in /var/lib/verde/settings.node). For example: VERDE_GATEWAY_CM_LIST=17.16.1.54; 17.16.1.88; 17.16.1.02.
Who is the master VERDE Management Console administrator?	Enter the VERDE Management Console system account user. For example, mcadmin1.
Is this a branch server?	Enter no regardless of whether this server will be a gateway for the core VERDE server or whether it will be a gateway for a branch server.
On which port should the VERDE Management Console and User Console run?	Enter 8443 or the port that will be used for https access to the User Console on the Isolated Gateway. Tomcat runs as a non-privileged user, so the port must be greater than 1024.
What character should be used to denote a space in user names?	Enter the default value of ^ or choose another character.
What local directory should be used for Read Cache I/O?	The following settings are used only when Read Cache I/O is enabled in the VERDE Management Console. Use the default value; the Isolated Gateway does not get cached GI copies because it does not host any VDI sessions.
How often should VDI nodes synchronize gold images from external storage (1-600 minutes)	The recommended value is 600 since the local cache copies are not used by the Isolated Gateway
What local directory should be used for Write Cache I/O?	Leave the default value (empty to use the users' home directories). The Isolated Gateway does not get cached copies of Gold Images since it does not host any VDI sessions.

## ACQUIRING A VERDE LICENSE

A free trial VERDE license is automatically provided upon successful registration of your installation.

When you first login as the VERDE Administrator you will be asked to register your VERDE installation. You may use an existing NComputing account or create a new one at this time.

After you have registered your installation the VERDE License management system will automatically enable the free trial license.

Contact the NComputing Global, Inc. sales team at [info@NComputing.com](mailto:info@NComputing.com) for more information about obtaining more licenses.

A detailed description of the license management system is described in the VERDE Administration and Management Guide



## Index

### B

Bare metal 20, 23

### C

Centos 20

Client

supported guest sessions 18

supported protocols 18

Cluster Master 22

Clustering Requirements 22

Common Installment Requirements 21

Copyright 2

CPU 15

virtual session calculation 6

### G

Gateway Server 21, 47

configuration settings 49

configure isolated gateway 47

preparation 48

requirements 47

Guest Session Support 18

Guest Sessions

disk assignments 14

### H

Hosting 21

### I

Installation

calculating memory requirements 5

CPU calculation 6

server capacity planning 5

using RPMs 29

cluster Master Candidate response  
file 45

configuration 30

configuration Script Questions 37

configuring the Branch Server 40

configuring VERDE environment 35

considerations 29

enable virtualization 30

installing 34

mounting shared storage 30

pre-installation configuration  
steps 31

running the Configuration Script in  
Menu Mode 42

running the Configuration Script in  
Unattended Mode 43

running the Unattended  
Installation 46

VDI Server response file 45

Installing VERDEOS 23

ISO file 23

## **L**

LDAP 21

Linux

    guest session support 19

    VERDE Server platforms 15

## **N**

NAS 20, 22

NComputing Management Portal 23

Network

    connection 26

    estimating bandwidth 12

    minimum and recommended  
        bandwidth 13

    planning considerations 12

Network Planning 12

Non-bare metal 20

NTP 22

## **O**

Open vSwitch Networking 26

## **P**

Platform Support

    NAS 9

Platforms, supported 15

## **Q**

Quick install 24

## **R**

RAM

    assignment for virtual sessions 5

    session and disk space planning 14

RDP

    bandwidth saving settings 13

Red Hat 20

RPM 15

RPM method 20-21

## **S**

SAN 22

Servers

    capacity planning

        optimization 7

        transient storage space with standard  
            deployment mode 8

    configuration 28

Sizing Per Desktops 10

Storage

    configuration 28

    long-life and static desktop  
        requirements 8

    shared storage planning 7-9

## T

trial license key 23

## U

Upgrading VERDE Requirements 22

## V

VERDE Cluster Master 21

VERDE Hosting 21

VERDE IMG 23

VERDE license 50

VERDE Menu 23

- access remotely 26

- navigating 25

- options 25

VERDE Server

- capacity planning 5

- CPU calculation 6

- memory considerations 5

- virtual desktop density 5, 7

VERDE VDI 22-23

- installing 23

VERDEOS 20, 22

- install the package 24