The TRELLIS™ Real-Time Infrastructure Optimization Platform

Pre-Installation

Installer/User Guide

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. Visit https://www.VertivCo.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

1 Preparing for the Installation **1**

1.1 Minimum Deployment Requirements 1

1.1.1 Workstation 2

1.1.2 TRELLIS™ platform 2

1.1.3 Microsoft® Windows® OS 4

1.1.4 Red Hat® Enterprise Linux® OS 5

1.2 Intelligence Engines 12

1.2.1 TRELLIS™ Intelligence Engine hardware requirements and pre-requisites 12

1.3 Installation Tools 14

1.4 Environment Details 15

1.5 Network Configuration 15

1.6 Firewall Ports 17

1.7 Firewall Security 20

1.8 Provisioning Requirements 20

1.9 Partitions, Disk Space and Permissions 21

1.9.1 Windows Disk Space Usage 22

1.9.2 Red Hat® Enterprise Linux® Directories Partitions and Disk Space 23

1.10 Authentication 24

1.10.1 Email Notification server assignments 25

1.11 Post Installation - Accessing the TRELLIS™ Platform Online Help File 25

2 Network Communication **26**

2.1 TRELLIS™ Intelligence Engine 26

2.2 Avocent® Universal Management Gateway Appliance 26

2.3 Ntegrity Gateway Appliance 26

2.3.1 Logical connections 26

2.3.2 Physical connections 27

2.4 Common Installation Scenarios 27

2.4.1 Installation on a network with the Ntegrity Gateway appliance 27

2.4.2 Installation on a separate private network for facility equipment 29

2.4.3 Configuring BACnet devices 32

2.4.4 Best practices for Virtual Machine (VM) environments 32

Appendices **34**

Appendix A: Browser Recommendations 34

Appendix B: Naming Conventions for Platform Domains 35

Appendix C: Red Hat® Enterprise Linux® OS Supported Time Zone List 36

1 PREPARING FOR THE INSTALLATION

The *Trellis*™ Real-Time Infrastructure Optimization Platform installation process is performed by our Professional Services team members. However, there are some activities that need to be performed by our customers before our team arrives. We have created this guide to help you prepare for our arrival and to ensure a successful *Trellis*™ platform installation.

This guide includes the minimum hardware and software requirements, instructions to install the operating system, special tools to be used during the installation and information that you need to provide to our team in advance of our arrival. General information includes network communication, environments and installation scenarios.

NOTE: In this guide, the word platform refers to the *Trellis*™ platform.

For additional information, please see the following guides:

- The TRELLIS™ Real-Time Infrastructure Optimization Platform User Guide
- The TRELLIS™ Real-Time Infrastructure Optimization Platform Red Hat® Enterprise Linux® (RHEL) Administrator's Guide
- The TRELLIS™ Real-Time Infrastructure Optimization Platform Microsoft® Windows® Administrator's Guide
- The TRELLIS™ Real-Time Infrastructure Optimization Platform Disaster Recovery Technical Bulletin
- Avocent® Universal Management Gateway Appliance Installer/User Guide

1.1 Minimum Deployment Requirements

The minimum requirements for the deployment of the *Trellis*™ platform software include a customer-supplied client workstation and two customer-supplied, dedicated server class machines, referred to as the front and back machines. The workstation and the front and back machines should be fully installed and equipped with the specified operating system, tools and provisioning requirements before the Professional Services team arrives to install the *Trellis™* platform software.

The workstation is used by the Professional Services team to perform the software installation and the server class machines are used to house the *Trellis*™ platform. The front machine hosts the application servers and the back machine hosts the database servers and services, such as authentication. Both the front and back machines must be accessible from the workstation.

NOTE: The *Trellis™* platform installers are delivered via the Content Delivery Network (CDN). Once downloaded, they must be extracted to the front and back machines or to a network share that is accessible from both machines.

NOTE: Make sure you are using a system that has the ability to share the installation configuration. For the following installation, an NFS/SMB system is used, which meets the sharing requirement.

NOTE: Vertiv™ supports the *Trellis*™ platform on physical and virtual server environments meeting the product documentation system specifications with dedicated system resources. While best performance is generally achieved in dedicated physical systems, virtual deployment can be effective as long as system resources are dedicated to the *Trellis™* platform Virtual Machine (VM) instance. For virtually hosted environments, Vertiv Technical Support will make every attempt to support any issues in the same manner that they would support the software in a physical server environment. Should an issue prove to be related exclusively to a virtually hosted environment, Vertiv Technical Support will make all appropriate recommendations to the customer for optimal operations; assistance may be required by the corresponding Virtual Host Solution Provider to fully resolve those environmental related issues.

The following sections provide the minimum deployment requirements for the workstation, *Trellis™* platform and the *Trellis*™ Intelligence Engine. For the machine and operating system requirements, see TRELLIS™ platform on page 2. For the hardware and operating system requirements, see Intelligence Engines on page 12.

1.1.1 Workstation

The following are the minimum hardware and software requirements for the workstation to facilitate installation of the *Trellis™* platform, version 5.0.1.1 and higher. These requirements are also applicable for the Bulk Data Processing tool. For more about the Bulk Data Processing tool, see Data Management in The TRELLIS™ Real-Time Infrastructure Optimization Platform User Guide.

Hardware

- Dual-core Intel® Pentium® 4 CPU at 2.8 GHz
- 8 GB RAM, LAN connection

Operating systems

- Microsoft® Windows® 7
- Red Hat® Enterprise Linux® version 6.7 and 6.10

Additional software

- Adobe® Flash® Player version 12 or higher
- Notepad++
- Microsoft® RDP Client (if installing the *Trellis*™ platform on Windows®)
- PuTTY (if installing the *Trellis™* platform on Red Hat® Enterprise Linux® or configuring the Avocent® Universal Management Gateway appliance)
- WinSCP (if installing the *Trellis™* platform on Red Hat® Enterprise Linux®)

Browsers for the *Trellis™* platform user interface

- Google Chrome™ version 40.0 to 63.0 and higher
- Microsoft Windows 10 Edge

Browsers for the symbol portal

- Google Chrome™ version 40.0 to 63.0 and higher

Browsers for 3D features

- Google Chrome™

NOTE: The recommended minimum screen resolution is 1280 x 1024.

For more information, see Browser Recommendations on page 34.

1.1.2 TRELLIS™ platform

The following are the minimum deployment requirements for the *Trellis™* platform, version 4.0.3 and higher.

Front and back machines

The following are minimum requirements on both the dedicated front and back machines to facilitate installation and operation of the *Trellis™* platform.

Table 1.1 Data Center Guidelines

COMPONENTS	SMALL	MEDIUM	LARGE	ENTERPRISE
Concurrent users	10	20	50	100
Devices	2,000	20,000	100,000	200,000
Power Connections	1,000	10,000	60,000	100,000
Data Connections	2,000	10,000	60,000	100,000
Monitored Datapoints	1,000	10,000	40,000	140,000
CPUs	2	4	4	4
CPU Cores	8	16	16	32

Table 1.2 Hardware Recommendations for the Front Machine

FRONT MACHINE HARDWARE	SMALL	MEDIUM	LARGE	ENTERPRISE
CPU manufacturer	Intel®	Intel®	Intel®	Intel®
CPU model	Xeon®	Xeon®	Xeon®	Xeon®
CPU speed (GHz) 8 M L3 cache	2.6	2.6	2.6	2.6
CPU count	1	2	2	2
CPU cores	4	4	4	8
Memory (GB) DDR3 1333 MHz	32	32	40	44
Disk throughput	> 500 MB/s (sequential) [uncached]			
Storage	300 GB Enterprise class			
Ethernet	> 80 MB/s			

Table 1.3 Hardware Recommendations for the Back Machine

BACK MACHINE HARDWARE	SMALL	MEDIUM	LARGE	ENTERPRISE
CPU manufacturer	Intel®	Intel®	Intel®	Intel®
CPU model	Xeon®	Xeon®	Xeon®	Xeon®
CPU speed (GHz) 8 M L3 cache	2.6	2.6	2.6	2.6
CPU count	1	2	2	2
CPU cores	4	4	4	8
Memory (GB) DDR3 1333 MHz	24	32	32	32
Disk throughput	> 500 MB/s (sequential) [uncached]			
Storage	*300 GB Enterprise class for base installation			
Ethernet	> 80 MB/s			

*Hardware sizing varies depending on usage requirements and is performed by Professional Services.

Operating systems

The *Trellis*™ platform supports the following operating systems and software. One of the following operating systems must be installed on both the front and back machines:

- Microsoft® Windows® Server 2012 R2
- Red Hat® Enterprise Linux® version 6.7 and 6.10

NOTE: Local administrative rights and remote desktop access are required to perform the *Trellis*™ platform installation.

NOTE: The front and back machine's operating system must have regional settings set to US English and the location set to United States.

NOTE: You must set the system locale to English US for both the front and back machines if the system locale is different than English US. Please refer to the operating system user guide for instructions on how to change the system locale.

1.1.3 Microsoft® Windows® OS

The full installation of the Windows operating system must be complete.

OS configuration

The OS configuration settings must be set up as follows for the installation directories, user configuration, security configuration and VM requirements.

Installation directories

The *Trellis*™ platform is installed to the C: drive by default. If you would like the platform installed to a different location, a symbolic link must be created to the following folders:

- c:\u01
- c:\u02
- c:\u03
- c:\u05

NOTE: *Trellis*™ platform Windows installers must be placed in c: drive folders and can no longer be run from folders that are defined as Symbolic links.

User configuration

All *Trellis*™ platform startups, shutdowns, installations, patches and upgrades must be performed using a Service Account with local Administrator privileges or by using the Administrator account.

NOTE: Always install, upgrade or patch the *Trellis*™ platform using the same Service Account.

Security configuration

The following are requirements for the configuration of security:

CAUTION: Disable any antivirus software prior to the installation of the *Trellis*™ platform. You can enable the antivirus software after completing the installation of the *Trellis*™ platform.

- Disable the Windows® firewall on all three profiles (domain, private and public) prior to the installation of the *Trellis*™ platform.
- Disable the automatic restart after Windows® updates.
- Always enable the UAC mode unless the installation is using the Administrator account.
- Restart the operating system after applying the UAC change.

VM requirements

The following VM platforms are supported when installing the *Trellis*™ platform in a virtual environment:

- Hyper-V 2012 R2 version 6.3 or higher (requires the Hyper-V Integration Services are installed on the guest operating system of the VMs that are housing the *Trellis*™ platform).
- VSphere version 4 or higher (requires all VMware tools are installed on the guest operating system of the VMs that are housing the *Trellis*™ platform).

1.1.4 Red Hat® Enterprise Linux® OS

The Linux operating system must be installed and provisioned for both the back and front machine using the supplied kickstart configuration file. The kickstart file ensures the operating system is ready for a successful *Trellis*™ platform installation.

You will receive the kickstart installation media from the Professional Services team before the scheduled date for OS provisioning or during the OS Requirements workshop.

NOTE: For Red Hat® Enterprise Linux® installations, it is important that the time zone is set to one of the supported time zones for the *Trellis*™ platform. See Red Hat® Enterprise Linux® OS Supported Time Zone List on page 36.

Using kickstart

After obtaining the kickstart file, it must be customized to reflect the network topology of the environment. Specifically, the IP address and identity of the front and back machines must be modified, as well as the passwords for both the root and oracle users.

If a customer wishes to use their own kickstart configuration file, the Linux® server administrator must incorporate all supplied kickstart file configuration settings into the operating system. Failure to do so could result in issues when running the *Trellis*™ platform installer.

CAUTION: Any changes to the supplied kickstart settings must be provided to the Professional Services team prior to installing the operating system, to allow time for assessment by the Engineering team. If any required configurations are absent, the installation may not be supported.

To locate and prepare the kickstart:

1. Copy the supplied *kickstart.cfg* file from the media to a location that can be reached by the front and back machines.
2. Open the *kickstart.cfg* file and edit the IP addresses, netmask, gateway and host filename for the machine on which the Red Hat® Enterprise Linux® operating system is to be installed. Then edit the root password and the oracle password.

CAUTION: Underscores are not supported in host filenames. The *Trellis*™ platform software requires a static IP. Changing the IP address after installation may render the software unusable.

To boot from the kickstart scripts to install the Red Hat® Enterprise Linux® libraries:

1. While booting at the virtual console of the back machine, press **F1**.

2. To make sure that distribution is supported, at the boot prompt enter linux rescue_ to boot off a USB and load the available drivers. Using this technique, you can confirm the names of the hard drives (usually /dev/sda) and the name of the network device. If the devices are not supported, you may need to follow the instructions provided by Red Hat® Enterprise Linux® to get the latest drivers for your hardware and make sure the distribution supports the hardware. See http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Installation_Guide/s1-kickstart2-startinginstall.html for more information.
3. To verify the devices are readable, enter the IP address, netmask and so on, for the back machine.

   Example: Back Machine Information

   linux ip=192.168.0.50 netmask=255.255.255.0 gateway=192.168.0.1 ksdevice=eth0 ks=nfs:192.168.0.1:/mnt/exports/front.cfg
4. While running the Anaconda installer, execute the kickstart scripts, then verify *Red Hat® Enterprise Linux® indicates up and booting* is displayed.
5. Repeat this procedure to install Red Hat® Enterprise Linux® on the front machine using another modified version of the kickstart scripts. Remember to enter the IP address for the front machine.

OS configuration

If not using the supplied kickstart file, the configuration settings must be set up as follows for the installation directories, users, groups, environment variables, additional files and services, sudoers content, system, required services and security.

Installation directories

The *Trellis*™ platform is installed to the root by default. If you would like the platform installed to a different location, a symbolic link must be created (as root) to the following folders:

- /u01
- /u02
- /u03
- /u05

NOTE: *Trellis*™ platform Windows installers must be placed in c: drive folders and can no longer be run from folders that are defined as Symbolic links.

User configuration

All *Trellis*™ platform startups, shutdowns, installations, patches and upgrades must be performed using the “oracle” user. The /etc/passwd file should have the oracle user and the SLI user set up and the home directory should be set to “/home/oracle:/bin/bash.”

The "runuser -l oracle -c 'umask'" command returns either 0000 or 0002.

Group configuration

Make sure the oinstall and dba groups in the /etc/group file are set up correctly. For the oracle/oinstall, make sure the users/user groups are configured as follows:

NOTE: The oracle user must be part of the oinstall and dba group.

- #create user and group
- /usr/sbin/groupadd oinstall
- /usr/sbin/groupadd dba

- /usr/sbin/useradd -g oinstall -G dba oracle
- /usr/sbin/usermod -g oinstall -G dba oracle
- id oracle

Environmental variables configuration

The following environmental variables should be set for the oracle user:

- PATH should contain /sbin/
- MW_HOME=/u01/fm/11.1.1.7/
- ORACLE_HOME=/u01/app/oracle/product/11.2.0
- ORACLE_SID=orcl

Additional required files

The following file exists with the following permissions set:

- /etc/oraInst.loc = -rw-r--r-- (root)

The /etc/oraInst.loc file contains the following lines:

- inventory_loc=/u01/app/oraInventory
- inst_group=oinstall

The following file exists with the following permissions set:

- /etc/oratab = -rw-rw-r-- (oracle:oinstall)

For Linux® 6.x ONLY, the following symlinks should be created and the files exist:

- libcrypto.so.1.0.0 -> /usr/lib/libcrypto.so.10
- libssl.so.1.0.0 -> /usr/lib/libssl.so.10

Additional services required

The /etc/xinetd.d/nodemanager file exists and content is identical to the following:

```
service nodemgrsvc
{
type = UNLISTED
disable = yes
socket_type = stream
protocol = tcp
wait = yes
user = root
port = 5556
flags = NOLIBWRAP
log_on_success += DURATION HOST USERID
server = /bin/su
server_args = - oracle -c /u01/trellis/startNodeManager.sh
}
```

Sudoers content

The "runuser -l oracle -c 'sudo -l' | grep "(root)" command lists out "(root) NOPASSWD:" for the following entries:

- /etc/init.d/trellis
- /u03/root/disable_escalation.sh
- /u03/root/enable_nodemanager.sh
- /u03/root/ohs_enable_chroot.sh
- /u03/root/postinstall_env_setup.sh
- /u03/root/preinstall_env_setup.sh
- /u03/root/sli_install.bin

NOTE: If this cannot be determined, the Sudoers file MUST match engineering specifications, as per the kickstart file.

System settings

The "/etc/sysctl.conf" file MUST contain the required parameters for the *Trellis*™ platform and should meet the following requirements:

- kernel.sem = "250 32000 100 128"
- net.ipv4.ip_local_port_range = "9000 65535"
- fs.aio-max-nr >= 1048576
- fs.file-max >= 6815744
- kernel.shmall >= 2097152
- kernel.shmmax >= 536870912
- kernel.shmmni >= 4096
- net.core.rmem_default >= 262144
- net.core.rmem_max >= 4194304
- net.core.wmem_default >= 262144
- net.core.wmem_max >= 1048586
- kernel.random.write_wakeup_threshold = 1024

The /etc/security/limits.conf file exists and content contains the following:

- oracle soft nproc 2047
- oracle hard nproc 16384
- oracle soft nofile 1024
- oracle hard nofile 65536
- oracle soft stack 10240

The /etc/pam.d/login file exists and content contains the following:

- session required /lib64/security/pam_limits.so

Required packages for Red Hat® Enterprise Linux® version 6.x and 7.x

The following are the required packages for Linux® version 6.x:

- mtools

- pax
- python-dmidecode
- kexec-tools
- fipscheck
- device-mapper-multipath
- sgpio
- emacs
- libsane-hpaio
- xorg-x11-utils
- xorg-x11-server-utils
- binutils
- compat-db
- compat-libcap1
- compat-libstdc++-33
- compat-libstdc++-33.i686
- device-mapper-multipath
- dos2unix
- elfutils-libelf
- elfutils-libelf-devel
- gcc
- gcc-c++
- glibc
- glibc.i686
- glibc-common
- glibc-devel
- glibc-devel.i686
- kexec-tools
- ksh
- libaio
- libaio.i686
- libaio-devel
- libaio-devel.i686
- libgcc
- libgcc.i686
- libsane-hpaio
- libstdc++
- libstdc++.i686
- libstdc++-devel
- libstdc++-devel.i686
- libXext
- libXi

- libXtst
- make
- openmotif
- openssl.i686
- redhat-lsb
- redhat-lsb-core.i686
- sgpio
- sysstat
- unixODBC
- unixODBC-devel
- xinetd.x86_64
- iptraf
- nmap
- screen
- strace

The following are the required packages for Red Hat® Enterprise Linux® version 7.x:

- mtools
- pax
- python-dmidecode
- kexec-tools
- fipscheck
- device-mapper-multipath
- sgpio
- emacs
- libsane-hpaio
- xorg-x11-utils
- xorg-x11-server-utils
- binutils
- compat-db
- compat-libcap1
- compat-libstdc++-33
- compat-libstdc++-33.i686
- device-mapper-multipath
- dos2unix
- elfutils-libelf
- elfutils-libelf-devel
- gcc
- gcc-c++
- glibc
- glibc.i686

- glibc-common
- glibc-devel
- glibc-devel.i686
- ksh
- libaio
- libaio.i686
- libaio-devel
- libaio-devel.i686
- libgcc
- libgcc.i686
- libsane-hpaio
- libstdc++
- libstdc++.i686
- libstdc++-devel
- libstdc++-devel.i686
- libXext
- libXi
- libXtst
- make
- motif
- redhat-lsb
- redhat-lsb-core.i686
- sgpio
- sysstat
- unixODBC
- unixODBC-devel
- xinetd.x86_64
- iptraf-ng
- nmap
- screen
- strace
- initscripts
- openssl-libs
- hdparm

NOTE: The Network Manager service should be disabled and the ANT package should NOT be installed.

Security configuration

The following are requirements for configuration of the operating system:

CAUTION: Disable any antivirus software prior to the installation of the *Trellis*™ platform. You can enable the antivirus software after completing the installation of the *Trellis*™ platform.

- Disable the Red Hat® Enterprise Linux® firewall (iptables) and SELinux.
- Make sure the RNGD service is set up to start with Red Hat® Enterprise Linux® to aid in the generation of entropy. This service is used to generate secure keys used by the *Trellis*™ platform during its execution and installation. Enabling this service dramatically improves the startup performance of systems that typically become starved for entropy.

NOTE: This is even more critical on virtual machines where the system does not generate entropy sufficiently. A hardware TRNG can be used and there are workarounds that offer lower quality entropy; however, use any workarounds with caution.

1.2 Intelligence Engines

With the *Trellis*™ Intelligence Engine, real-time communications are possible within the solution. The data collection engine is responsible for polling and collecting data from all the managed elements in a data center. The Intelligence Engine can be installed on Red Hat® Enterprise Linux® or Ubuntu operating systems on a standalone server or in a virtual environment.

Two versions of the *Trellis*™ Intelligence Engine are available. One engine is provided with the *Trellis*™ Site Manager module and the other engine is embedded in the Avocent® Universal Management Gateway appliance. Their functionality is explained in the *Trellis*™ Real-Time Infrastructure Optimization Platform User Guide.

1.2.1 TRELLIS™ Intelligence Engine hardware requirements and pre-requisites

The Intelligence Engine is supported in *Trellis*™ platform version 4.0.3 and higher. The *Trellis™* Intelligence Engine packages for Red Hat® Enterprise Linux® and Ubuntu OS are included in the front and back machine installations.

The following are the minimum deployment requirements for the *Trellis™* Intelligence Engine.

Table 1.4 *Trellis*™ Intelligence Engine Hardware Requirements

SPECIFICATION	DATAPOINTS PER MINUTE				
	10000	20000	30000	40000	50000
CPU Manufacturer	Intel®	Intel®	Intel®	Intel®	Intel®
CPU Model	Xeon®	Xeon®	Xeon®	Xeon®	Xeon®
CPU Speed (GHz) 8M L3 Cache	2.4	2.4	2.4	2.4	2.4
CPU Count	1	1	1	1	1
CPU Cores (per CPU)	2	3	3	4	4
Memory (GB) DDR3 1333 MHz	2	3	3	4	5
Disk Throughput	500 MB/s (sequential) [uncached]				
Storage	25 GB*	35 GB*	35 GB*	50 GB*	50 GB*
Ethernet	>50 MB/s				

* No local backup.

The required packages and dependencies to install the *Trellis™* Intelligence Engine are handled by the installer. The only pre-requisites are the following:

For both Red Hat® Enterprise Linux® and Ubuntu, if the root user is not available, a user with sudo permissions is required to install the *Trellis™* Intelligence Engine.

Red Hat® Enterprise Linux® requirements are:

- Must have access to the Red Hat® Enterprise Linux® 7.x and EPEL repositories. If the box/VM has internet connection, and Linux® is registered, you have access to it.
- If there is no access, the following packages must be installed by the System Administrator prior to running the *Trellis™* Intelligence Engine installer:
  - net-tools
  - psmisc
  - net-snmp
  - openssl
  - postgresql
  - postgresql-contrib
  - postgresql-server
  - glibmm24
- The following packages are from the EPEL repo:
  - Log4cpp
  - Jsoncpp
  - Libpqxx

Ubuntu requirements are:

Access to the Ubuntu 14.04.x repositories is required. If the box/VM has an internet connection, you can access the repositories.

If there is no access, the following packages must be installed by the System Administrator prior to running the *Trellis*™ Intelligence Engine installer:

- postgresql
- postgresql-contrib
- liblog4cpp5
- libpqxx-4.0
- snmp
- snmpd
- libsigx-2.0-2
- syslog-ng-core
- syslog-ng

Performance tuning

The following *Trellis™* Intelligence Engine configuration changes are recommended for instances of the embedded PostgreSQL database where data is collected at 30000 datapoints per minute and higher.

1. Log into the *Trellis™* Intelligence Engine host operating system via SSH using PuTTY or a similar program.
2. For Red Hat® Enterprise Linux®, enter **/var/lib/pgsql/intelligence-engine/postgresql.conf** to open the postgresql.conf file.

-or-

For Ubuntu, enter **/etc/postgresql/9.3/intelligence-engine/postgresql.conf**.

3. Using a "vi" editor or similar, enable the following PostgreSQL configuration settings and then adjust the corresponding configuration values as listed:

NOTE: Remove the # symbol for the following configuration settings.

- shared_buffers = 256
- checkpoint_segments = 32
- checkpoint_completion_target = 0.9
- wal_buffers = 16
- temp_buffers = 8 MB
- commit_delay = 10000
- work_mem = 16 MB
- maintenance_work_mem = 16 MB
- checkpoint_timeout = 30 min

4. For Red Hat®™ Enterprise Linux®™, execute the following commands for the configuration settings to take effect immediately:
   - systemctl enable postgresql-ie
   - systemctl stop postgresql-ie
   - systemctl start postgresql-ie

   -or-

   For Ubuntu, execute the following commands:

   - /etc/init.d/postgresql stop
   - /etc/init.d/postgresql start

Supported host environments

The *Trellis*™ Intelligence Engine can be installed on VM Ware, Hyper V or a physical machine.

Supported operating systems

The following are the supported operating systems for the *Trellis™* Intelligence Engine:

- Red Hat® Enterprise Linux® 7.2, 64-bit
- Ubuntu 14.04 LTS (release 14.04.1 and 14.04.3), 64-bit

Supported PostgreSQL databases

The following PostgreSQL databases are installed with the *Trellis™* Intelligence Engine:

- Red Hat® Enterprise Linux® 7.2 – PostgreSQL 9.2
- Ubuntu 14.04 LTS (release 14.04.1 and 14.04.3) – PostgreSQL 9.3

1.3 Installation Tools

To facilitate the installation process, the following tools must be in place on your customer-supplied workstation:

- PuTTY (if installing on Red Hat® Enterprise Linux® and/or planning on upgrading firmware on the Avocent® Universal Management Gateway appliance, to access the front and back machines using SSH via port 22)
- Notepad ++ enhanced text editor (useful if installing on Linux)
- WinSCP (if installing on Linux)
- Windows Sysinternals Toolkit must be installed prior to installation. (Installation is performed by the Professional Services team.)
- PDF Reader and Microsoft Word (to open our installation instructions and copy and paste commands)
- Remote desktop access to both machines (if installing on Windows)

NOTE: Your customer-supplied workstation is not required if the Professional Services team is able to use their workstation to access the *Trellis*™ platform machines while on-site.

1.4 Environment Details

The following information must be provided to the Professional Services team before and during the installation process:

- IP addresses and fully qualified domain names for the front and back machines. See Naming Conventions for Platform Domains on page 35.
- Red Hat® Enterprise Linux® root password (or log in as root) or Administrator password for Windows at various points during installation
- Oracle user password (supplied by your Red Hat® Enterprise Linux® administrator when editing the supplied kickstart file)
- Domain and mail server information (to access your SMTP mail server to send mail and to set up new user accounts)

1.5 Network Configuration

The following are requirements for network configuration:

- Permanent IPv4/IPv6 addresses are required for both of the *Trellis™* platform machines (front and back). DHCP is supported as long as the *Trellis™* platform machines are given specifically reserved IP addresses with permanent leases. Changing the IP address on any of the *Trellis™* platform machines after installation causes the application to stop functioning.
- Only one NIC can be enabled for the installation of the *Trellis™* platform.
- Only one routable IPv4 address can be present/enabled on each platform machine during installation. If there are multiple NIC addresses, they must be teamed so that there is only one routable IP address for the platform machine. Multi-homing is not supported.
- Prior to installation the hosts file (or DNS) must be changed to include the *Trellis*™ platform entries. ALL required hosts names resolve to the correct IP on both the front and back machines.

NOTE: The installation media contains an example configuration for reference.

NOTE: For Windows, entries may be ignored if there are too many entries on any single line of the hosts file. This is an OS limitation.

The front hosts are as follows:

- <FRONT_FQDN>
- <FRONT_HOSTNAME>
- weblogic-admin
- Presentation-Operational-internal

- Presentation-Analytical-internal
- BAM-internal
- SOA-Operational-internal
- SOA-Analytical-internal
- MPS-proxy-internal
- CEP-Engine-internal
- OHS-Balancer-internal
- OSB-Server-internal
- Authentication-internal
- Authorization-internal-local
- Flexera-Server-internal
- vip-external
- 3rdparty-vip-external
- vip-internal
- MPS-proxy-external
- Search-internal
- Reporting-internal
- trellis-front
- trellis-platform

The back hosts are as follows:

- <BACK_FQDN>
- <BACK_HOSTNAME>
- MDS-Database-internal
- CDM-Database-internal
- TSD-Database-internal
- TSD-Database-external
- Authorization-internal-admin
- trellis-back

- The time server and time zone on the front and back machines should match. In addition, the date and time should match on both machines.

NOTE: For Windows installations, this can be omitted if the servers are Domain joined because they receive time from the Active Directory via NTP.

NOTE: For Red Hat® Enterprise Linux® installations, it is important that the time zone is set to one of the supported time zones. Professional Services can supply a list of supported time zones for the *Trellis*™ platform.

- It is also important to verify that none of the *Trellis™* platform ports are used by any other running services (see the firewall ports list).
- The *Trellis*™ platform machines should be able to "ping" each other and should return an RTT with 1 hop and < 10 ms RTT.
- The transfer speed between the machines should be > 30 MB/s.

1.6 Firewall Ports

The following tables provide source and destination components, protocols and ports for the *Trellis™* Intelligence Engine and the engine embedded in the Avocent® Universal Management Gateway appliance.

Table 1.5 *Trellis™* Intelligence Engine Firewall Ports

SOURCE	DESTINATION	PROTOCOL	TRANSPORT	PORT	NOTES
loopback	loopback	N/A	N/A	N/A	Configure loopback to ACCEPT: loopback 127.0.0.1/32
Trellis Platform Front Server (OHS)	Intelligence Engine (Linux)	HTTPS	TCP	4440	Communication is one direction and is over two-way SSL
Intelligence Engine (Linux)	*Trellis* Front Machine	HTTPS	TCP	6443	Communication is one direction and is over two-way SSL
Administrator Workstation	Linux	SSH	TCP	22	Installation/maintenance access
Intelligence Engine	Target Devices	SNMP	UDP	161	Default port; Set/Get operation; requires customer confirmation
		Modbus	TCP	502	Default port; requires customer confirmation
		OPC UA	TCP	21381	Default port; requires customer confirmation
		BACNet	UDP	47808	Default port; requires customer confirmation
		Velocity (Vertiv protocol)	UDP	47808	Default port; requires customer confirmation
		Telnet	TCP	23	Default port; requires customer confirmation
Target Devices	Intelligence Engine (Linux)	Velocity and BACNet	UDP	47777-48117	For BACNet/IP and Velocity return traffic
SNMP traps	Intelligence Engine	SNMP	UDP	162	SNMP Traps
Intelligence Engine	PostgreSQL (Internal)	PostgreSQL	TCP	4321	PostgreSQL database Admin
Service Processors	Service Processor Manager (SPM)	IPMI	TCP	623	N/A
		Telnet	TCP	23	Default port
		HTTPS	TCP	443	Used for discovery
		HTTP	TCP	80	Used for discovery
		SSH	TCP	23	Default port
		N/A	UDP	623	Return IPMI traffic
Service Processor Manage	Service Processors	N/A	IPMI	50000-59999	SP access
Service Processor Manager	Redis Server (Internal)	RESP	TCP	6379	Message transportation between SPM processes
Service Processor Manager	PostreSQL (Internal)	PostgreSQL	TCP	4322	SPM PostgreSQL database Admin

Table 1.6 Firewall Configuration

DIRECTION	INTERFACE	SOURCE	DESTINATION	SERVICE	ACTION	USE-CASE RECOMMENDATIONS
Input	Any	Any	Any	SNMP Trap (162)	Allow	Used to monitor SNMP devices for the Intelligence Engine
Input	Any	Any	Any	Front machine (OHS 6443)	Allow	Used for *Trellis* platform management and monitoring support
Input	Any	Any	Any	Intelligence Engine (4440)	Allow	Used by the Intelligence Engine for management and monitoring support of the *Trellis* platform
Input	Any	Any	Any	Velocity and BACNet Incoming	Allow	Used to monitor BACNet over IP devices for the Intelligence Engine
Input	Any	Any	Any	Modbus	Allow	Used to monitor Modbus over IP devices for the Intelligence Engine
Input	Any	Any	Any	OPC UA	Allow	Used to monitor OPC UA over IP devices for the Intelligence Engine
Input	Any	Any	Any	SNMP	Allow	Used to monitor SNMP over IP devices for the Intelligence Engine
Input	Any	Any	Any	BACNet	Allow	Used to monitor SNMP over IP devices for the Intelligence Engine
Input	Any	Any	Any	Velocity (Vertiv protocol)	Allow	Used to monitor Velocity (Vertiv protocol) devices for the Intelligence Engine

Table 1.7 Embedded Intelligence Engine Firewall Ports

SOURCE	DESTINATION	PROTOCOL	TRANSPORT	PORT	NOTES
Web Browser	Front Machine	HTTPS	TCP	443	Secure Web UI access.
Web Browser	Appliance OBWI	HTTPS	TCP	443	Secure Web UI access.
		HTTP	TCP	843	Web UI Data - Flash.
		HTTP	TCP	8123	Web UI Data - XML.
		HTTP	TCP	8080	Upload the SSL cert, download the backup of the Avocent® Universal Management Gateway appliance and so on.
		HTTPS	TCP	443	Secure Web UI access.
Administrator Workstation	Front Machine (Linux)	SSH	TCP	22	Installation/maintenance access.
	Back Machine (Linux)	SSH	TCP	22	Installation/maintenance access.
	Appliance	SSH	TCP	22	Installation/maintenance access.
	Front Machine (Windows)	RDP	TCP	3389	Remote desktop - Installation/maintenance access.
	Back Machine (Windows)	RDP	TCP	3389	Remote desktop - Installation/maintenance access.
	Front Machine (Windows)	N/A	N/A	N/A	File copy - Installation/maintenance access.
	Back Machine (Windows)	N/A	N/A	N/A	File copy - Installation/ maintenance access.
Front Machine	Back Machine	ICMP	N/A	N/A	Health check - ping.
		TCP	TCP	7	Installation (Jasper) Host validation.
		JDBC	TCP	1521	Database.
		LDAP	TCP	7023	Security.
		LDAP	TCP	7026	Security.
		LDAPS	TCP	7027	Security.
		TS3	TCP	7031	Security (SSL).
		HTTP	TCP	8080	Entitlement.
		SSH	TCP	22	Installation/maintenance access.
	Back Machine Windows Only	RDP	TCP	3389	Remote desktop - Installation/maintenance access.
	Back Machine Windows Only	N/A	N/A	N/A	File copy - Installation/maintenance access.
Back Machine	Front Machine	SSH	TCP	22	Installation/maintenance access.
	Front Machine	ICMP	N/A	N/A	Health check (ping).
	Front Machine Windows Only	RDP	TCP	3389	Remote desktop - Installation/maintenance access.
	Front Machine Windows Only	N/A	N/A	N/A	File copy - Installation/maintenance access.
Front Machine	Appliance	HTTPS	TCP	4440	Communication is one direction but over 2-way SSL.
Trellis Intelligence	Front Machine	HTTPS	TCP	6443	Communication is one direction but over 2-way

SOURCE	DESTINATION	PROTOCOL	TRANSPORT	PORT	NOTES
Engine and Appliance		N/A	TCP	8012	SSL. Port used instead of 6443 only if upgraded from *Trellis*™ 2.0.x.
Trellis Intelligence Engine and Appliance	Target Devices	SNMP	UDP	161	Set/Get operation, default port; requires customer confirmation.
		BACNet/IP	UDP	47808	Default port; requires customer confirmation.
		Velocity/IP	UDP	47808	Default port; requires customer confirmation.
		OPC UA	TCP	21381	Default port for Matrikon OPC UA Wrapper; default ports for other vendors can differ; requires customer confirmation.
		Modbus	TCP	502	Default port; requires customer confirmation.
Target Devices	Appliance	SNMP	UDP	162	SNMP traps.
		N/A	UDP	47777-48117	For BACNet/IP and Velocity return traffic.
Trellis Intelligence Engine and Appliance	Service Processors	IPMI	UDP	623	Default port for IPMI.
		Telnet	TCP	23	Default port for Telnet.
		SSH	TCP	22	Default port for SSH.
		HTTP	TCP	80	Used for discovery.
		HTTPS	TCP	443	Used for discovery.
Service Processors	Appliance	N/A	UDP	623	Return IPMI traffic.

1.7 Firewall Security

Firewall management is extremely resource intensive and requires a high skill level. Because of the effort and complexity involved, a majority of firewall breaches are caused by insufficient firewall rules and policies.

Firewall security is the responsibility of the customer. A top level security policy is essential to any serious security scheme. The policy should outline rules for computer network access, determine how policies are enforced and lay out some of the basic architecture of the company security/network security environment. For your policy, see the National Institute for Standards and Technology for security guidelines.

1.8 Provisioning Requirements

The following are the rack U space, power and network requirements for the *Trellis*™ platform components.

Table 1.8 Space Provisioning Requirements

DEVICE	RACK U SPACE REQUIRED
Trellis platform front and back machines	Based on models
Ntegrity Gateway (NG) appliance	1U
Avocent Universal Management Gateway appliance	1U

Table 1.9 Power Provisioning Requirements

DEVICE	POWER REQUIREMENTS
Trellis platform front and back machines	Based on models
Ntegrity Gateway appliance	1 x 120-220V power supply
Avocent Universal Management Gateway appliance	2 x 120-220V power supplies

Table 1.10 Physical Network Connectivity Provisioning Requirements

DEVICE	NETWORK REQUIREMENTS
Trellis platform front and back machines	Based on hardware
Ntegrity Gateway appliance	1x (optional)
Avocent Universal Management Gateway appliance	- 1x corporate LAN (choose 1; 1x empty, 1x teamed corporate LAN, 1x management LAN, 1x private facilities LAN) - 1x patch cable to MPU (may be direct or through patch panel)

1.9 Partitions, Disk Space and Permissions

NOTE: The following directory structure is representative of post-install utilization; all shown directories are created as part of the installation process. It is not necessary to create the following structures prior to installation.

While the following tables indicate the minimum disk requirement for the application is 300 GB for each server-class machine, the actual disk usage depends on a number of factors, including quantity of data collected and duration of data retention for historical purposes. The following tables illustrate typical disk utilization and are provided as a guideline for planning disk capacity for the *Trellis*™ platform front and back machines.

The minimum disk requirements are for installation purposes only and do not include data collected, duration of data collected or the retention of the data for historical purposes. Please work with the Vertiv Professional Services team to plan appropriate disk space for data collection.

1.9.1 Windows Disk Space Usage

Table 1.11 Windows Front Machine Application Servers

DIRECTORY	MINIMUM SPACE REQUIRED	OWNERSHIP/ PERMISSIONS	CONTENT NOTES
C:\Users\Administrator	20 GB	administrator	Working directory for installation, upgrades and patching. Examples are: C:\Users\Administrator\AppData\Local\Temp\2 and C:\Users\Administrator\TrellisScripts.zip 10 + GB.
c:\bea\homelist	0.001 GB	administrator	Inventory file for WebLogic installation and patching.
c:\u01	24 GB	administrator	Oracle Tech Stack log files. 99% read only. Logs start at less than 10 GB, but allocate 24 GB for future upgrades of Tech Stack to support log captures and other support-related activities. The execution of capture_ logs.cmd places the system state in a zip or jar file in the c:\u01\trellis directory. These small logs are rarely used.
c:\u02	120 GB	administrator	Application Domain/IDM/OHS configuration. Logs start at 7 GB and can grow to 80 GB within six months on an active system. Also, 40 GB are reserved to support patching and support related activities.
c:\u03	5 GB	administrator	Installer logs. In future versions the logs are increased in this location with total space for c:\u02 and c:\u03 remaining the same; c:\u02 space becomes less as logs are placed in c:\u03.
c:\windows\.....	10 GB	administrator	Windows system registry and supporting service initialization.
%CUSTOMER_SPECIFIC_ LOCATION% Windows ISOs	20 GB	administrator	Windows ISOs may be removed after installation of the *Trellis* platform or after an upgrade. Vertiv currently uses c:\u05 directly internally by convention, but this is customer specific. Space must be allocated for each upgrade and patch.
%CUSTOMER_SPECIFIC_ LOCATION% Binaries	20 GB	administrator	Binaries may be removed after installation of the *Trellis* platform or after an upgrade. Vertiv currently uses c:\u05 directly internally by convention, but this is customer specific. Space must be allocated for each upgrade and patch.
Reserve	80 GB	N/A	Reserved for contingency.
Total	299.001 GB	N/A	N/A

Table 1.12 Windows® Back Machine Database Servers

DIRECTORY	MINIMUM SPACE REQUIRED	OWNERSHIP/ PERMISSIONS	CONTENT NOTES
C:\Users\Administrator	20	administrator	Working directory for installation, upgrades and patching: C:\Users\Administrator\AppData\Local\Temp\2; C:\Users\Administrator\TrellisScripts.zip 10 + GB
c:\bea\homelist	0.001	administrator	Inventory file for WebLogic installation and patching.
c:\u01	60 GB	administrator	Oracle Tech Stack log files start at less than 10 GB, but 24 GB are allocated to support future upgrades of Tech Stack for log captures and other support related activities. Execution of capture_logs.cmd places the system state in a zip or jar file in the c:\u01\trellis directory. c:\u01\app\oracle\admin\orcl\dpdump\ contains schema backups.
c:\u02	110 GB	administrator	IDM Domain / Database. Starts at 7 GB and can grow to 80 GB within six months on an active system. Also, 40 GB are reserved to support patching and support-related activities. Database files are stored in c:\u02\app\oracle\oradata\orcl\ grow by design. Calculations must be refined during a sizing exercise.
c:\u03	5 GB	administrator	Installer logs; In future versions of the platform, the logs are increased in this location and totals for the c:\u02 location and c:\u03 location are the same, but the c:\u02 space becomes less as logs are placed in c:\u03.
C:\Program Files\Vertiv\	0.2 GB	administrator	License supporting components.
C:\Program Files\Oracle\	0.1 GB	administrator	Oracle Tech Stack inventory and logs of inventory changes.
c:\windows\.....	10 GB	administrator	Windows System Registry and supporting service configuration; 10 GB is aggressive.
%CUSTOMER_SPECIFIC_ LOCATION%\WindowsISOs	20 GB	administrator	Windows ISOs may be removed after the installation of the *Trellis* platform or after an upgrade. Vertiv currently uses c:\u05 directly internally by convention, but this is customer specific. Space must be allocated for each upgrade and patch.
%CUSTOMER_SPECIFIC_ LOCATION%\Binaries	20 GB	administrator	Binaries may be removed after installation of the *Trellis* platform or after an upgrade. Vertiv currently uses c:\u05 directly internally by convention, but this is customer specific. Space must be allocated for each upgrade and patch.
%FULL_BACKUP_LOCATION% %ARCHIVE_LOGS_ DIRECTORY%	5 GB	administrator	Calculations must be refined during the sizing exercise. Generally, this is four times the size of the weekly database backup to be stored and not purged by the *Trellis* platform. Growth depends on the frequency of backups and size of the overall database, as with any log file.
Reserve	80 GB	N/A	Reserved for contingency.
Total	295.301	N/A	N/A

1.9.2 Red Hat® Enterprise Linux® Directories Partitions and Disk Space

You may choose to represent the Linux® directories that are required by the *Trellis*™ platform as separate partitions. While this should not introduce any issues with installation, the size of these partitions/directories must be adequate for the installation process. The following table provides requirements for the Linux server team to follow when configuring the directory partitions for the servers on the front and back machines.

Table 1.13 Server Directory Partition Requirements

DIRECTORY	MINIMUM SPACE REQUIRED	OWNERSHIP/ PERMISSIONS	CONTENT NOTES
/home/oracle	20 GB	oracle / drwxrwxr-x	Working directory for installation, upgrades and patching; /home/oracle/TrellisScripts.zip 10 + GB profile information.
/tmp	10 GB	root / drwxrwxr-x	/tmp is used during installation; some temp files are placed here during runtime and removed when the server is shut down properly.
/u01	24 GB	oracle / drwxrwxr-x	Oracle Tech Stack; 99% read-only log files starting at less than 10 GB, but 24 GB is allocated for future upgrades of Tech Stack to support log captures and other support related activities; these small logs are rarely used.
/u02	60 GB	oracle / drwxrwxr-x	Application Domain/IDM Domain/Database/OHS configuration. Logs start at 7 GB and can grow to 80 GB within six months on an active system. Also, 40 GB are reserved to support patching and support related activities.
/u03	5 GB	oracle / drwxrwxr-x	Installer logs; in future releases these logs are increased in this location and the \u02 location and \u03 location totals remain the same, but the \u02 space becomes less as logs are placed in \u03.
/u05	24 GB	oracle / drwxrwxr-x	Location for the extracted *Trellis* platform installation binaries; used internally by convention as a location to install non-product monitoring services.
/	10 GB	root / drwxr-xr-x	/etc gets populated with scripts to manage the *Trellis* platform and Oracle servers.
Reserve	145 GB	N/A	Reserved for contingency.
Total	298	N/A	N/A

1.10 Authentication

In addition to one local administrative account, the *Trellis*™ platform supports the following types of user authentication.

- Local user authentication
- Active Directory (AD)
- LDAP

If AD authentication is configured during installation, the Professional Services team needs the following platform information to locate and authenticate users:

- Host: IP address of the domain controller (not the host name)
- Port: TCP port 636 for SSL Mode or TCP port 389 for standard LDAP
- Root: Example - dc=tac,dc=pro
- Base DN, Group Base DN and User Base DN: example dc=tac,dc=pro
- Type: *ACTIVE_DIRECTORY* or *LDAP*
- SSL Mode: Enabled checkbox (use TCP Port 636) or disabled checkbox (use TCP Port 389)
- Access Credentials: Use full username; example cn=Bind,cn=Users,dc=tac,dc=pro

NOTE: Without access credentials, the added external authentication provider may not function as desired.

- Use Chasing Referrals: Enabled or disabled checkbox

1.10.1 Email Notification server assignments

The Email Notification server must be assigned in order to send temporary log in credentials after a user is created. Temporary passwords are auto generated using the local policy for complexity.

To set up the email notification server to send log in credentials:

1. In the *Trellis*™ platform UI, click the Administration icon and select *Notification Settings*.
2. Scroll to and complete the Email Server and SMS Server panel fields.

1.11 Post Installation - Accessing the TRELLIS™ Platform Online Help File

The help file for the *Trellis™* platform is available via the Internet. Customers without Internet access or not wanting to expose the *Trellis™* platform servers to the Internet, can download the *Trellis™* platform Online Help file for local access. When using a local copy, if you reinstall or upgrade the *Trellis™* platform software, the location to access the help file resets to the online location and requires resetting to the local source.

To access the *Trellis™* platform Online Help file from the Internet:

1. In the *Trellis*™ platform UI, click the Administration icon and select *System Settings*.
2. In the Summary panel, select the Vertiv™ Web Site radio button and click *Save*.

To download and install the Online Help file for local access:

1. Using a server with Internet access, visit http://www.VertivCo.com/.
2. Click *The TRELLIS™ Real-Time Infrastructure Optimization Platform Online Help* and select *Trellis™ Platform Online Help.zip File*.
3. Using a USB drive or CD ROM, copy and transfer the .zip file to the front machine.
4. In the *Trellis™* platform UI, click the Administration icon and select *System Settings*.
5. In the Summary panel, select the *Trellis*™ Server radio button.
6. Click SELECT FILE, navigate to and select the previously downloaded .zip file, and in the UI, click *Download*.

2 NETWORK COMMUNICATION

Different aspects and options must be considered when installing the *Trellis*™ platform on a network, both externally and internally.

The application servers must be able to communicate externally with Vertiv™ entitlement servers during installation and any time licensing or entitlement is changed. SSL-secured communications use port 443 from the application servers to access: https://VertivCo.com.

Internally, application servers may communicate with each other and with Universal Management Gateway appliances when one or more appliances are part of the platform and reside on the same network and/or subnet. A key strength of the platform is this ability to connect to a vast array of infrastructure devices to gather information. Connectivity is primarily provided by the *Trellis*™ Intelligence Engine, Avocent® Universal Management Gateway appliance or the Liebert® Ntegrity Gateway appliance.

Communication with devices is via public or private networks or via physical connections. Each engine/appliance has two main network ports, eth0 and eth1, and at least one of these two ports must be able to communicate on a LAN network to the application servers.

Each engine/appliance supports physical and logical connections to target devices.

NOTE: Only one engine/appliance is allowed to be connected to and monitor a target device at the same time.

2.1 TRELLIS™ Intelligence Engine

For an overview of the *Trellis™* Intelligence Engine, see Intelligence Engines on page 12.

2.2 Avocent® Universal Management Gateway Appliance

The Avocent® Universal Management Gateway is an optional multi-purpose appliance that offers consolidated access to facility and IT equipment, making it possible for data centers to execute a unified approach to infrastructure management, and resulting in greatly reduced cost and more efficient management and control. The appliance solves problems in the data center infrastructure management (DCIM) market by providing both real-time data and closed loop control to the *Trellis™* platform solution. Within DCIM, remote data center management (RDCM) is defined as IT access and control.

2.3 Ntegrity Gateway Appliance

The Ntegrity Gateway appliance is an optional secure hardware appliance that resides within the enterprise private network to collect information from devices being monitored and provide remote access to other *Trellis™* platform hardware. This is a very useful tool in situations where customer support is required, allowing Vertiv Technical Support to access the *Trellis™* platform hardware to assist with upgrades or other support related matters.

For more information about appliances, please contact your sales person.

2.3.1 Logical connections

Targets connected to an appliance logically are available via network access, which has several options.

Service processor (SP) targets

SPs may be logically connected to an appliance using an SP sub-network, or they can be connected logically or physically via appliance target ports.

SP sub-network

The appliance may be connected to the SP sub-network using the eth1 port of the appliance. This setup is recommended when OEM tools, such as HP, SIM or IBM Director, are already being used and must also have network access to the SPs.

Logical connections via appliance target ports

The appliance may connect to SPs logically or physically via one or more of the target ports, if the ports are connected to a customer network. Each SP in this configuration requires a dedicated appliance target port.

Monitoring targets

To monitor targets via a logical network connection, one of the two dedicated Ethernet ports on the appliance, eth0 or eth1, must be connected to that network.

2.3.2 Physical connections

Targets must be connected to one of the target ports on the back of the appliance. Different appliance models have different port configurations.

KVM

When supported, a KVM target requires use of a UMIQ module and must be connected to the appliance by an Ethernet cable with a total length not longer than 100 m.

CAUTION: Never connect a network switch, hub, firewall, router or anything, between an appliance and a UMIQ module. Appliances send electricity that damages anything that is not a UMIQ module.

Other targets, such as the SP or serial console

NOTE: Depending on the appliance model, other targets may be physically connected to the proper appliance ports. Monitoring of facilities equipment, such as PDUs or UPSes, is only supported via logical network connections.

2.4 Common Installation Scenarios

Various options are available when deploying the *Trellis*™ platform with the Avocent® Universal Management Gateway and Ntegrity Gateway appliances. The Avocent® Universal Management Gateway appliance is placed behind the firewall. The Ntegrity Gateway appliance may be placed in a DMZ or behind a firewall. For deployment scenarios using the Ntegrity Gateway appliance behind a firewall, see Installation on a Network Without Facilities on page 28. Facilities equipment within the data center may reside on a corporate network or on a private network. For scenarios where facilities equipment is on the corporate network, see Installation on a Network Without Facilities on page 28 and Installation on a Separate Private Network for Facility Equipment on page 30. For an example of devices on a private network, see Installation on a Separate Private Network for Facility Equipment on page 30.

2.4.1 Installation on a network with the Ntegrity Gateway appliance

In this scenario, the platform is installed on the front and back machines, which are accessed by a user with a web browser on the same corporate LAN. The Ntegrity Gateway appliance is behind a firewall communicating to Vertiv™ via a secure connection. The Avocent® Universal Management Gateway appliance is on the same corporate LAN as the platform machines, monitoring physical target devices such as power strips and PDUs on that same network. Some devices may also be physically connected to ports on the back of the Avocent® Universal Management Gateway appliance.

Figure 2.1 Installation on a Network Without Facilities

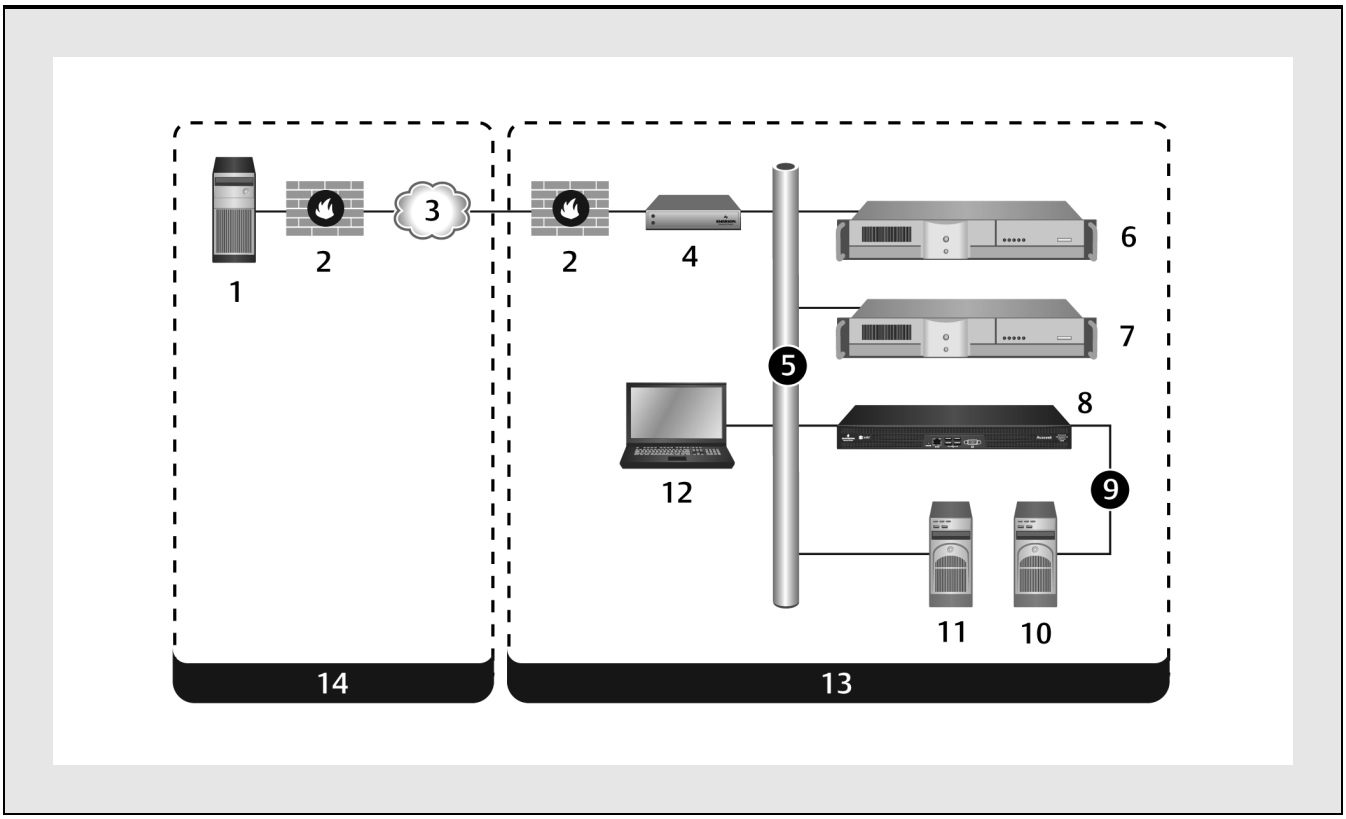

Table 2.1 Installation on a Network without Facilities

ITEM	NAME	DESCRIPTION
1	Vertiv Controlled Access Server	Provides network security enforcement
2	Firewall	Prevents unauthorized access to or from a private network
3	Internet	Global system of interconnected networks
4	Ntegrity Gateway (NG) appliance	Ensures the security of a network
5	LAN	Computer network that interconnects computers within a limited area
6	*Trellis* platform front machine	Software platform production system front end
7	*Trellis* platform back machine	Software platform production system back end
8	Avocent Universal Management Gateway appliance/ *Trellis* Intelligence Engine	Enables remote management of devices
9	Serial Over Ethernet	Allows for sharing a serial port over the network (Internet or LAN)
10	Physical Target Devices	Represents the physical target devices
11	Logical Target Devices	Represents the logical target devices
12	Users	The *Trellis*™ platform users
13	Unencrypted Local Traffic	Local traffic that is unencrypted
14	Encrypted Network Traffic	Network traffic that is encrypted

2.4.2 Installation on a separate private network for facility equipment

In this scenario, the Ntegrity Gateway appliance sits behind a firewall and facilities equipment is logically connected on a private facilities LAN. To access the private LAN, the Avocent® Universal Management Gateway appliance is dual-homed. Some devices may also be physically connected to the ports on the appliance.

Figure 2.2 Installation on a Separate Private Network for Facility Equipment

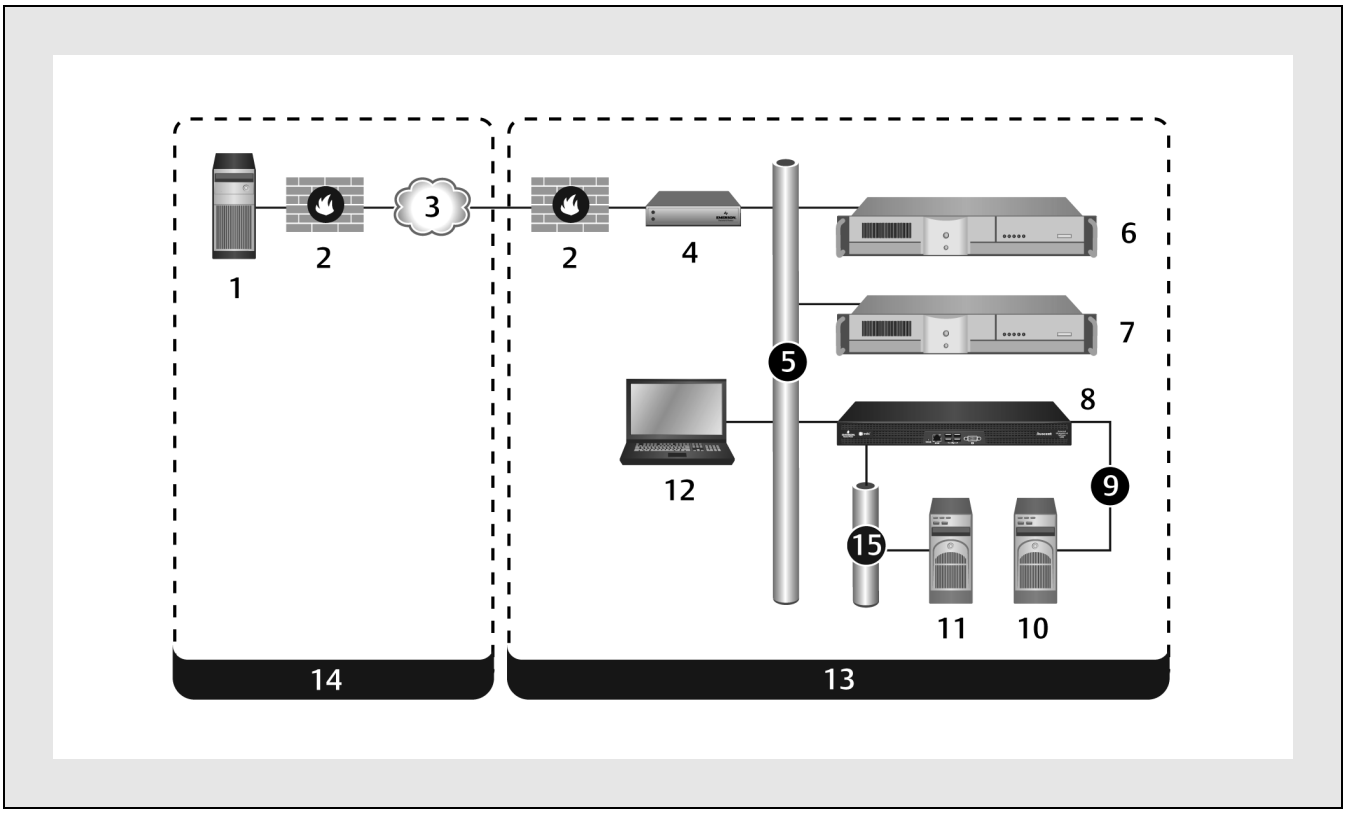

Table 2.2 Installation on a Network with Facilities

ITEM	NAME	DESCRIPTION
1	Vertiv Controlled Access Server	Provides network security enforcement
2	Firewall	Prevents unauthorized access to or from a private network
3	Internet	Global system of interconnected networks
4	Ntegrity Gateway (NG) appliance	Ensures the security of a network
5	Corporate LAN	Computer network that interconnects computers within a limited area
6	*Trellis* platform front machine	Software platform production system front end
7	*Trellis* platform back machine	Software platform production system back end
8	Avocent Universal Management Gateway appliance	Enables remote management of devices
9	Serial Over Ethernet	It should be noted that this is only a sample and assumes that the backup location provides an ssh interface, and allows for the exchange of SSH keys
10	Logical Target Devices	Represents the logical target devices
11	Physical Target Devices	Represents the physical target devices
12	Users	The *Trellis* platform users
13	Unencrypted Local Traffic	Local traffic that is unencrypted
14	Encrypted Network Traffic	Network traffic that is encrypted
15	Facilities LAN	Provides a computer network that interconnects computers within a specific area

Table 2.3 Installation on a Network with Facilities

ITEM	NAME	DESCRIPTION
1	Vertiv Controlled Access Server	Provides network security enforcement
2	Firewall	Prevents unauthorized access to or from a private network
3	Internet	Global system of interconnected networks
4	Ntegrity Gateway (NG) appliance	Ensures the security of a network
5	Corporate LAN	Computer network that interconnects computers within a limited area
6	*Trellis* platform front machine	The software platform production system front end
7	*Trellis* platform back machine	The software platform production system back end
8	Avocent Universal Management Gateway appliance	Enables remote management of devices
9	Serial Over Ethernet	It should be noted that this is only a sample and assumes that the backup location provides an ssh interface, and allows for the exchange of SSH keys
10	Logical Target Devices	Represents the logical target devices
11	Physical Target Devices	Represents the physical target devices
12	Users	The *Trellis* platform users
13	Unencrypted Local Traffic	Local traffic that is unencrypted
14	Encrypted Network Traffic	Network traffic that is encrypted
15	Facilities LAN	Provides a computer network that interconnects computers within a specific area

2.4.3 Configuring BACnet devices

When an appliance such as SiteLink™, is monitoring Building Automation and Control Networks (BACnet) devices, and it is on a different IP subnet than the subnet that the Avocent® Universal Management Gateway appliance is on, the IP address of the SiteLink™ appliance needs to be added to the BBMD (BACnet Broadcast Management Device) table for the BACnet router on that IP subnet.

A SiteLink™ appliance is always a BACnet device and can also be a BACnet router. For SiteScan™, one SiteLink™ per subnet is automatically configured as a BACnet router (or BBMD) when the system is built. That is how SiteScan™ (an IP-based system, often on a separate subnet from one or more SiteLink™ appliances) works.

When adding the appliance to the network, this BACnet router SiteLink™ requires the IP address of the appliance to be appended in its BBMD table. If the appliance is accessing other SiteLink™ appliances on the same subnet, which were not originally BBMD routers, those SiteLink™ appliances may also need to be forced to act as a BBMD. BACnet should function with only one BBMD per subnet, which acts as a router for all other BACnet devices on the subnet. The *Trellis*™ platform supports this by allowing you to enter the IP address of both the monitored SiteLink™ appliance and the appropriate BBMD router. For SiteLink™ appliances that are also configured as BBMD routers, both of these addresses are the same.

There are ways to update the existing BBMD tables on SiteLink™ hardware through SiteScan™, as well as using separate software tools. These are generally proprietary/vendor-specific.

NOTE: Customers may have BACnet systems that are not SiteScan™/SiteLink™ devices.

2.4.4 Best practices for Virtual Machine (VM) environments

The following best practices help ensure optimal performance when running the *Trellis™* platform in a virtual environment.

- If power management is enabled on the host machine BIOS, disable it, then in the processor settings, disable *C-States* and *C1E* and set the power management settings to *Maximum Performance*.

- Always use the minimum recommended resources in the *Trellis* platform VMs.

NOTE: Depending on the density of the cluster that is housing the *Trellis*™ platform, if there is a high vCPU/pCPU ratio on the hosts, we have seen CPU ready times > 200-300 ms cause a drop in performance. For this, we recommend adding more hosts to counteract CPU contention. If this is not possible, we have seen a considerable drop in CPU contention and better performance when dropping the VMs from four vCPUs to two vCPUs.

- If resources are overallocated, or if there is contention, make sure to have the VMs in a resource pool with high memory/CPU shares and set reservations when possible.
- When taking a snapshot of the *Trellis*™ platform VMs, make sure the platform services are stopped or the VMs are powered off to ensure the VMs are in sync for the snapshot and to avoid failures due to high amounts of I/O traffic.
- Do not run VMs that are housing the *Trellis™* platform on snapshots for extended periods of time. The delta files can grow rapidly due to the amount of I/O in the *Trellis* platform. This also decreases read/write speeds and causes performance degradation.
- If you are using Distributed Resources Scheduler (DRS) and the VM network traffic becomes a bottleneck, set affinity rules to keep the front and back VMs on the same host.

APPENDICES

Appendix A: Browser Recommendations

The following are general recommendations pertaining to the supported browsers:

- If on-screen data is not updating correctly, clear the browser cache.
- If security certificate warnings are displayed while using an https connection to access the *Trellis*™ platform, ignore the warning and proceed to access the site.
- Disable pop-up blockers.
- If accessing graphical pages, use Adobe Flash Player version 12.0 or higher.
- When importing or exporting data using Internet Explorer, select *Tools - Internet Options - Advanced*, then under the HTTP 1.1 settings section, deselect *Use HTTP 1.1*.

Appendix B: Naming Conventions for Platform Domains

When assigning a domain name to the *Trellis*™ platform, the following are required:

NOTE: The *Trellis*™ platform domain name is not an FQDN name.

- The domain name should be alphanumeric with no spaces or special characters.
- If the name begins with t, b, n, r or f, the initial character must be capitalized to prevent the name from being confused with various specific commands/sequences in the software.
- If running multiple *Trellis*™ platform instances on the same network segment, each *Trellis*™ platform domain name must be unique.
- The domain name should begin with an alpha character and have 16 or less characters in the name. The following are examples of acceptable names:
    - TrellisDomain
    - TrellisPROD
    - TrellisLIVE
    - TrellisDEV
    - TrellisTEST
    - TrellisDEVDomain

Appendix C: Red Hat® Enterprise Linux® OS Supported Time Zone List

The following are the Linux OS Supported Time Zones.

Table 5.1 Linux OS Supported Time Zones

Africa/Addis_Ababa	Africa/Lubumbashi	America/Argentina/San_Luis
Africa/Abidjan	Africa/Lusaka	America/Argentina/Tucuman
Africa/Accra	Africa/Malabo	America/Argentina/Ushuaia
Africa/Algiers	Africa/Maputo	America/Aruba
Africa/Asmara	Africa/Maseru	America/Asuncion
Africa/Asmera	Africa/Mbabane	America/Atikokan
Africa/Bamako	Africa/Mogadishu	America/Atka
Africa/Bangui	Africa/Monrovia	America/Bahia
Africa/Banjul	Africa/Nairobi	America/Barbados
Africa/Bissau	Africa/Ndjamena	America/Belem
Africa/Blantyre	Africa/Niamey	America/Belize
Africa/Brazzaville	Africa/Nouakchott	America/Blanc-Sablon
Africa/Bujumbura	Africa/Ouagadougou	America/Boa_Vista
Africa/Cairo	Africa/Porto-Novo	America/Bogota
Africa/Casablanca	Africa/Sao_Tome	America/Boise
Africa/Ceuta	Africa/Timbuktu	America/Buenos_Aires
Africa/Conakry	Africa/Tripoli	America/Cambridge_Bay
Africa/Dakar	Africa/Tunis	America/Campo_Grande
Africa/Dar_es_Salaam	Africa/Windhoek	America/Cancun
Africa/Djibouti	America/Adak	America/Caracas
Africa/Douala	America/Anchorage	America/Catamarca
Africa/El_Aaiun	America/Anguilla	America/Cayenne
Africa/Freetown	America/Antigua	America/Cayman
Africa/Gaborone	America/Araguaina	America/Chicago
Africa/Harare	America/Argentina/Buenos_Aires	America/Chihuahua
Africa/Johannesburg	America/Argentina/ Catamarca	America/Coral_Harbour
Africa/Kampala	America/Argentina/ ComodRivadavia	America/Cordoba
Africa/Khartoum	America/Argentina/Cordoba	America/Costa_Rica
Africa/Kigali	America/Argentina/Jujuy	America/Cuiaba
Africa/Kinshasa	America/Argentina/La_Rioja	America/Curacao
Africa/Lagos	America/Argentina/Mendoza	America/Danmarkshavn
Africa/Libreville	America/Argentina/Rio_Gallegos	America/Dawson
Africa/Lome	America/Argentina/Salta	America/Dawson_Creek
Africa/Luanda	America/Argentina/San_Juan	America/Denver

America/Detroit	America/Knox_IN	America/Porto_Velho
America/Dominica	America/La_Paz	America/Puerto_Rico
America/Edmonton	America/Lima	America/Rainy_River
America/Eirunepe	America/Los_Angeles	America/Rankin_Inlet
America/El_Salvador	America/Louisville	America/Recife
America/Fort_Wayne	America/Maceio	America/Regina
America/Fortaleza	America/Managua	America/Resolute
America/Glace_Bay	America/Manaus	America/Rio_Branco
America/Godthab	America/Marigot	America/Rosario
America/Goose_Bay	America/Martinique	America/Santiago
America/Grand_Turk	America/Mazatlan	America/Santo_Domingo
America/Grenada	America/Mendoza	America/Sao_Paulo
America/Guadeloupe	America/Menominee	America/Scoresbysund
America/Guatemala	America/Merida	America/Shiprock
America/Guayaquil	America/Mexico_City	America/St_Barthelemy
America/Guyana	America/Miquelon	America/St_Johns
America/Halifax	America/Moncton	America/St_Kitts
America/Havana	America/Monterrey	America/St_Lucia
America/Hermosillo	America/Montevideo	America/St_Thomas
America/Indiana/Indianapolis	America/Montreal	America/St_Vincent
America/Indiana/Knox	America/Montserrat	America/Swift_Current
America/Indiana/Marengo	America/Nassau	America/Tegucigalpa
America/Indiana/Petersburg	America/New_York	America/Thule
America/Indiana/Tell_City	America/Nipigon	America/Thunder_Bay
America/Indiana/Vevay	America/Nome	America/Tijuana
America/Indiana/Vincennes	America/Noronha	America/Toronto
America/Indiana/Winamac	America/North_Dakota/Center	America/Tortola
America/Indianapolis	America/North_Dakota/New_Salem	America/Vancouver
America/Inuvik	America/Panama	America/Virgin
America/Iqaluit	America/Pangnirtung	America/Whitehorse
America/Jamaica	America/Paramaribo	America/Winnipeg
America/Jujuy	America/Phoenix	America/Yakutat
America/Juneau	America/Port_of_Spain	America/Yellowknife
America/Kentucky/Louisville	America/Port-au-Prince	Antarctica/Casey
America/Kentucky/Monticello	America/Porto_Acre	Antarctica/Davis

Antarctica/DumontDUrville	Asia/Ho_Chi_Minh	Asia/Riyadh
Antarctica/Mawson	Asia/Hong_Kong	Asia/Saigon
Antarctica/McMurdo	Asia/Hovd	Asia/Sakhalin
Antarctica/Palmer	Asia/Irkutsk	Asia/Samarkand
Antarctica/South_Pole	Asia/Istanbul	Asia/Seoul
Antarctica/Syowa	Asia/Jakarta	Asia/Shanghai
Arctic/Longyearbyen	Asia/Jayapura	Asia/Singapore
Asia/Aden	Asia/Jerusalem	Asia/Taipei
Asia/Almaty	Asia/Kabul	Asia/Tashkent
Asia/Amman	Asia/Kamchatka	Asia/Tbilisi
Asia/Anadyr	Asia/Karachi	Asia/Tehran
Asia/Aqtau	Asia/Kashgar	Asia/Tel_Aviv
Asia/Aqtobe	Asia/Kathmandu	Asia/Thimbu
Asia/Ashgabat	Asia/Katmandu	Asia/Thimphu
Asia/Ashkhabad	Asia/Kolkata	Asia/Tokyo
Asia/Baghdad	Asia/Krasnoyarsk	Asia/Ujung_Pandang
Asia/Bahrain	Asia/Kuala_Lumpur	Asia/Ulaanbaatar
Asia/Baku	Asia/Kuching	Asia/Urumqi
Asia/Bangkok	Asia/Kuwait	Asia/Vientiane
Asia/Beirut	Asia/Macao	Asia/Vladivostok
Asia/Bishkek	Asia/Macau	Asia/Yakutsk
Asia/Brunei	Asia/Magadan	Asia/Yekaterinburg
Asia/Calcutta	Asia/Makassar	Asia/Yerevan
Asia/Choibalsan	Asia/Manila	Atlantic/Azores
Asia/Chongqing	Asia/Muscat	Atlantic/Bermuda
Asia/Chungking	Asia/Nicosia	Atlantic/Canary
Asia/Colombo	Asia/Novosibirsk	Atlantic/Cape_Verde
Asia/Dacca	Asia/Omsk	Atlantic/Faeroe
Asia/Damascus	Asia/Oral	Atlantic/Faroe
Asia/Dhaka	Asia/Phnom_Penh	Atlantic/Jan_Mayen
Asia/Dili	Asia/Pontianak	Atlantic/Madeira
Asia/Dubai	Asia/Pyongyang	Atlantic/Reykjavik
Asia/Dushanbe	Asia/Qatar	Atlantic/South_Georgia
Asia/Gaza	Asia/Qyzylorda	Atlantic/St_Helena
Asia/Harbin	Asia/Rangoon	Atlantic/Stanley

Australia/ACT	Canada/Yukon	Etc/GMT-4
Australia/Adelaide	CET	Etc/GMT-5
Australia/Brisbane	Chile/Continental	Etc/GMT-6
Australia/Broken_Hill	Chile/EasterIsland	Etc/GMT-7
Australia/Canberra	CST6CDT	Etc/GMT-8
Australia/Currie	Cuba	Etc/GMT-9
Australia/Darwin	EET	Etc/Greenwich
Australia/Eucla	Egypt	Europe/Amsterdam
Australia/Hobart	Eire	Europe/Andorra
Australia/LHI	EST	Europe/Athens
Australia/Lindeman	EST5EDT	Europe/Belfast
Australia/Lord_Howe	Etc/GMT	Europe/Belgrade
Australia/Melbourne	Etc/GMT+0	Europe/Berlin
Australia/North	Etc/GMT+1	Europe/Bratislava
Australia/NSW	Etc/GMT+10	Europe/Brussels
Australia/Perth	Etc/GMT+11	Europe/Bucharest
Australia/Queensland	Etc/GMT+12	Europe/Budapest
Australia/South	Etc/GMT+2	Europe/Chisinau
Australia/Sydney	Etc/GMT+3	Europe/Copenhagen
Australia/Tasmania	Etc/GMT+4	Europe/Dublin
Australia/Victoria	Etc/GMT+5	Europe/Gibraltar
Australia/West	Etc/GMT+6	Europe/Guernsey
Australia/Yancowinna	Etc/GMT+7	Europe/Helsinki
Brazil/Acre	Etc/GMT+8	Europe/Isle_of_Man
Brazil/DeNoronha	Etc/GMT+9	Europe/Istanbul
Brazil/East	Etc/GMT0	Europe/Jersey
Brazil/West	Etc/GMT-0	Europe/Kaliningrad
Canada/Atlantic	Etc/GMT-1	Europe/Kiev
Canada/Central	Etc/GMT-10	Europe/Lisbon
Canada/Eastern	Etc/GMT-11	Europe/Ljubljana
Canada/East-Saskatchewan	Etc/GMT-12	Europe/London
Canada/Mountain	Etc/GMT-13	Europe/Luxembourg
Canada/Newfoundland	Etc/GMT-14	Europe/Madrid
Canada/Pacific	Etc/GMT-2	Europe/Malta
Canada/Saskatchewan	Etc/GMT-3	Europe/Mariehamn

Europe/Minsk	GMT-0	Pacific/Efate
Europe/Monaco	Greenwich	Pacific/Enderbury
Europe/Moscow	Hongkong	Pacific/Fakaofo
Europe/Nicosia	HST	Pacific/Fiji
Europe/Oslo	Iceland	Pacific/Funafuti
Europe/Paris	Indian/Antananarivo	Pacific/Galapagos
Europe/Podgorica	Indian/Chagos	Pacific/Gambier
Europe/Prague	Indian/Christmas	Pacific/Guadalcanal
Europe/Riga	Indian/Cocos	Pacific/Guam
Europe/Rome	Indian/Comoro	Pacific/Honolulu
Europe/Samara	Indian/Kerguelen	Pacific/Johnston
Europe/San_Marino	Indian/Mahe	Pacific/Kiritimati
Europe/Sarajevo	Indian/Maldives	Pacific/Kosrae
Europe/Simferopol	Indian/Mauritius	Pacific/Kwajalein
Europe/Skopje	Indian/Mayotte	Pacific/Majuro
Europe/Sofia	Indian/Reunion	Pacific/Marquesas
Europe/Stockholm	Iran	Pacific/Midway
Europe/Tallinn	Israel	Pacific/Nauru
Europe/Tirane	Jamaica	Pacific/Niue
Europe/Tiraspol	Japan	Pacific/Norfolk
Europe/Uzhgorod	Kwajalein	Pacific/Noumea
Europe/Vaduz	Libya	Pacific/Pago_Pago
Europe/Vatican	MET	Pacific/Palau
Europe/Vienna	Mexico/BajaNorte	Pacific/Pitcairn
Europe/Vilnius	Mexico/BajaSur	Pacific/Ponape
Europe/Volgograd	Mexico/General	Pacific/Port_Moresby
Europe/Warsaw	MST	Pacific/Rarotonga
Europe/Zagreb	MST7MDT	Pacific/Saipan
Europe/Zaporozhye	Navajo	Pacific/Samoa
Europe/Zurich	NZ	Pacific/Tahiti
GB	NZ-CHAT	Pacific/Tarawa
GB-Eire	Pacific/Apia	Pacific/Tongatapu
GMT	Pacific/Auckland	Pacific/Truk
GMT+0	Pacific/Chatham	Pacific/Wake
GMT0	Pacific/Easter	Pacific/Wallis

Pacific/Yap
Poland
Portugal
PRC
PST8PDT
ROC
ROK
Singapore
Turkey
US/Alaska
US/Aleutian
US/Arizona
US/Central
US/Eastern
US/East-Indiana
US/Hawaii
US/Indiana-Starke
US/Michigan
US/Mountain
US/Pacific
US/Samoa
UTC
WET
W-SU

VertivCo.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

© 2019 Vertiv Co. All rights reserved. Vertiv and the Vertiv logo are trademarks or registered trademarks of Vertiv Co. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness herein, Vertiv Co. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications are subject to change without notice.

590-1541-501F