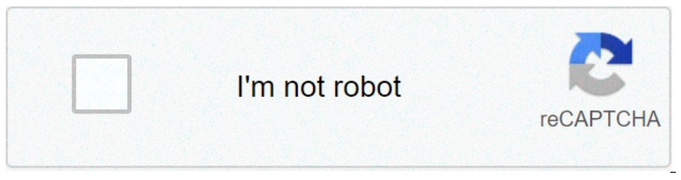

Continue

Ntp server time sync

Google Public NTP serves leap-smeared time. We use this technology to smoothly handle leap seconds with no disruptive events. We implemented Google Public NTP with our load balancers and our fleet of atomic clocks in data centers around the world. Zentyal integrates ntpd [2] as its NTP server. NTP uses UDP port 123. Zentyal uses the NTP server to both, synchronize its own clock and offer this service on the network. It's generally recommended to install and enable this service in most deployments. Once you have enabled the module, you can check in that it is running and that the option to manually adjust the time is disabled. You still need to configure your time zone. NTP module installed and enabled If you access to , you can enable or disable the service and choose the external servers that you want to synchronize to. By default the list has already three preconfigured servers chosen from the NTP project [3]. NTP configuration and external servers Once Zentyal is synchronized, you can offer your clock timing using the NTP service, generally, through DHCP. As always, you must not forget to check the firewall rules, keeping in mind that NTP is usually enabled only for internal networks. Applies to SUSE Linux Enterprise Server 12 SP525 Time Synchronization with NTP # The NTP (network time protocol) mechanism is a protocol for synchronizing the system time over the network. First, a machine can obtain the time from a server that is a reliable time source. Second, a machine can itself act as a time source for other computers in the network. The goal is twofold—maintaining the absolute time and synchronizing the system time of all machines within a network. Maintaining an exact system time is important in many situations. The built-in hardware clock does often not meet the requirements of applications such as databases or clusters. Manual correction of the system time would lead to severe problems because, for example, a backward leap can cause malfunction of critical applications. Within a network, it is usually necessary to synchronize the system time of all machines, but manual time adjustment is a bad approach. NTP provides a mechanism to solve these problems. The NTP service continuously adjusts the system time with reliable time servers in the network. It further enables the management of local reference clocks, such as radio-controlled clocks. 25.1 Configuring an NTP Client with YaST # The NTP daemon (ntpd) coming with the ntp package is preset to use the local computer clock as a time reference. Using the hardware clock, however, only serves as a fallback for cases where no time source of better precision is available. YaST simplifies the configuration of an NTP client. 25.1.1 Basic Configuration # The YaST NTP client configuration (›) consists of tabs. Set the start mode of ntpd and the server to query on the tab. Select , if you want to manually start the ntpd daemon. Select to set the system time periodically without a permanently running ntpd. You can set the . Select to start ntpd automatically when the system is booted. This setting is recommended. 25.1.2 Changing Basic Configuration # The servers and other time sources for the client to query are listed in the lower part of the tab. Modify this list as needed with , , and . provides the possibility to view the log files of your client. Click to add a new source of time information. In the following dialog, select the type of source with which the time synchronization should be made. The following options are available: Figure 25.1: YaST: NTP Server #Server In the drop-down list (see Figure 25.1, “YaST: NTP Server”), determine whether to set up time synchronization using a time server from your local network () or an Internet-based time server that takes care of your time zone (). For a local time server, click to start an SLP query for available time servers in your network. Select the most suitable time server from the list of search results and exit the dialog with . For a public time server, select your country (time zone) and a suitable server from the list under then exit the dialog with . In the main dialog, test the availability of the selected server with . allows you to specify additional options for ntpd. Using , you can restrict the actions that the remote computer can perform with the daemon running on your computer. This field is enabled only after checking on the tab (see Figure 25.2, “Advanced NTP Configuration: Security Settings”). The options correspond to the restrict clauses in /etc/ntp.conf. For example, nomodify notrap noquery disallows the server to modify NTP settings of your computer and to use the trap facility (a remote event logging feature) of your NTP daemon. Using these restrictions is recommended for servers out of your control (for example, on the Internet). Refer to /usr/share/doc/packages/ntp-doc (part of the ntp-doc package) for detailed information. Peer A peer is a machine to which a symmetric relationship is established: it acts both as a time server and as a client. To use a peer in the same network instead of a server, enter the address of the system. The rest of the dialog is identical to the dialog. Radio Clock To use a radio clock in your system for the time synchronization, enter the clock type, unit number, device name, and other options in this dialog. Click to fine-tune the driver. Detailed information about the operation of a local radio clock is available in /usr/share/doc/packages/ntp-doc/refclock.html. Outgoing Broadcast Time information and queries can also be transmitted by broadcast in the network. In this dialog, enter the address to which such broadcasts should be sent. Do not activate broadcasting unless you have a reliable time source like a radio controlled clock. Incoming Broadcast If you want your client to receive its information via broadcast, enter the address from which the respective packets should be accepted in this fields. Figure 25.2: Advanced NTP Configuration: Security Settings # In the tab (see Figure 25.2, “Advanced NTP Configuration: Security Settings”), determine whether ntpd should be started in a chroot jail. By default, is not activated. The chroot jail option increases the security in the event of an attack over ntpd, as it prevents the attacker from compromising the entire system. increases the security of your system by disallowing remote computers to view and modify NTP settings of your computer and to use the trap facility for remote event logging. After being enabled, these restrictions apply to all remote computers, unless you override the access control options for individual computers in the list of time sources in the tab. For all other remote computers, only querying for local time is allowed. Enable if SuSEFirewall2 is active (which it is by default). If you leave the port closed, it is not possible to establish a connection to the time server. 25.2 Manually Configuring NTP in the Network # The easiest way to use a time server in the network is to set server parameters. For example, if a time server called ntp.example.com is reachable from the network, add its name to the file /etc/ntp.conf by adding the following line: To add more time servers, insert additional lines with the keyword server. After initializing ntpd with the command systemctl start ntp, it takes about one hour until the time is stabilized and the drift file for correcting the local computer clock is created. With the drift file, the systematic error of the hardware clock can be computed when the computer is powered on. The correction is used immediately, resulting in a higher stability of the system time. There are two possible ways to use the NTP mechanism as a client: First, the client can query the time from a known server in regular intervals. With many clients, this approach can cause a high load on the server. Second, the client can wait for NTP broadcasts sent out by broadcast time servers in the network. This approach has the disadvantage that the quality of the server is unknown and a server sending out wrong information can cause severe problems. If the time is obtained via broadcast, you do not need the server name. In this case, enter the line broadcastclient in the configuration file /etc/ntp.conf. To use one or more known time servers exclusively, enter their names in the line starting with servers. 25.3 Setting Up a Local Reference Clock # The software package ntpd contains drivers for connecting local reference clocks. A list of supported clocks is available in the ntp-doc package in the file /usr/share/doc/packages/ntp-doc/refclock.html. Every driver is associated with a number. In NTP, the actual configuration takes place by means of pseudo IP addresses. The clocks are entered in the file /etc/ntp.conf as though they existed in the network. For this purpose, they are assigned special IP addresses in the form 127.127.T.U. Here, T stands for the type of the clock and determines which driver is used and U for the unit, which determines the interface used. Normally, the individual drivers have special parameters that describe configuration details. The file /usr/share/doc/packages/ntp-doc/drivers/driverNN.html (where NN is the number of the driver) provides information about the particular type of clock. For example, the “type 8” clock (radio clock over serial interface) requires an additional mode that specifies the clock more precisely. The Conrad DCF77 receiver module, for example, has mode 5. To use this clock as a preferred reference, specify the keyword prefer. The complete server line for a Conrad DCF77 receiver module would be: server 127.127.8.0 mode 5 prefer Other clocks follow the same pattern. Following the installation of the ntp-doc package, the documentation for NTP is available in the directory /usr/share/doc/packages/ntp-doc. The file /usr/share/doc/packages/ntp-doc/refclock.html provides links to the driver pages describing the driver parameters. 25.4 Clock Synchronization to an External Time Reference (ETR) # Support for clock synchronization to an external time reference (ETR) is available. The external time reference sends an oscillator signal and a synchronization signal every 2**20 (2 to the power of 20) microseconds to keep TOD clocks of all connected servers synchronized. For availability two ETR units can be connected to a machine. If the clock deviates for more than the sync-check tolerance all CPUs get a machine check that indicates that the clock is out of sync. If this happens, all DASD I/O to XRC enabled devices is stopped until the clock is synchronized again. The ETR support is activated via two sysfs attributes; run the following commands as root: echo 1 > /sys/devices/system/etr/etr0/online echo 1 > /sys/devices/system/etr/etr1/online The most straightforward method to synchronize to a time server is to use the Windows net time command. If you connect to a Novell server, your computer's clock is automatically updated. At Indiana University, you must be logged into the ADS domain on the IU network (via either a direct or VPN connection) before you can synchronize to IU's time server. To use the net time command: Navigate to an elevated command prompt. At the command prompt, enter: net time \\ads.iu.edu /set /y At the command prompt, enter exit to return to Windows. Possible errors and solutions Occasionally, you will see one or more of the following error messages when attempting the net time command: System error 5 System error 53 has occurred Network path not found If you get one of these error messages, try the following solutions: Re-enter the net time command. Repeat the steps above. There are many reasons why net time may fail to synchronize with a time server the first time (for example, there may be too many concurrent server requests). If you've entered the command immediately after your computer booted up, it may not have had enough time to load all of the necessary Windows components. Verify that you have permission to use that network's time server. For example, to use IU's time server, you must first log into the ADS domain. If you are not connected to the IU network, you will be rejected when you attempt to synchronize to ads.iu.edu. Other networks have different rules for access; consult the administrators of the network you wish to synchronize to. Alternate method for synchronizing your computer's clock to IU's time server Navigate to an elevated command prompt. At the command prompt, enter: w32TM /config /syncfromflags:manual /manualpeerlist:ntp.indiana.edu Enter: w32tm /config /update Enter: w32tm /resync At the command prompt, enter exit to return to Windows. NIST Internet Time Servers Return to NIST Internet Time Service Page NOTICE: NIST has established a mailing list (Google Group) to inform users of status changes of the Internet Time Service. If you wish to subscribe to this list, please send your name and email address to: internet-time-service@nist.gov The table below lists the time servers used by the NIST Internet Time Service (ITS). The table lists each server's name, IP address, and location, organized geographically within the US from North to South and then from East to West. Please note that while we make every effort to ensure that the names of the servers are correct, we control the names of only the nist.gov servers. If you have difficulty using the name of a system, you can access a server using the IP address directly. Important notes: 1. We will continue to support the "TIME" protocol that uses tcp port 37 for the forseeable future. However, this protocol is very expensive in terms of network bandwidth, since it uses the complete tcp machinery to transmit only 32 bits of data. Users are *strongly* encouraged to upgrade to the network time protocol (NTP), which is both more accurate and more robust. 2. Users of the NIST "DAYTIME" protocol on tcp port 13 are also strongly encouraged to upgrade to the network time protocol, which provides greater accuracy and requires less network bandwidth. The NIST time client (nistime-32bit.exe) supports both protocols. 3. The generic name time.nist.gov will continue to point to all of our servers on a round-robin basis, and users are encouraged to access the service using this name. Please address comments to: internet-time-service@nist.gov The global address time.nist.gov is resolved to all of the server addresses below in a round-robin sequence to equalize the load across all of the servers. Whether you connect to a server using the name or the IP address, it is a bad practice to “hard-code” a particular server name or address into a device so that these parameters cannot be changed by the end user if that becomes necessary at some future time. All users should ensure that their software NEVER queries a server more frequently than once every 4 seconds. Systems that exceed this rate will be refused service. In extreme cases, systems that exceed this limit may be considered as attempting a denial-of-service attack. Name IP Address Location Status time-a-g.nist.gov 129.6.15.28 NIST, Gaithersburg, Maryland All services available time-b-g.nist.gov 129.6.15.29 NIST, Gaithersburg, Maryland All services available time-c-g.nist.gov 129.6.15.30 NIST, Gaithersburg, Maryland All services available time-d-g.nist.gov 129.6.15.27 NIST, Gaithersburg, Maryland All services available time-d-g.nist.gov 2610:20:6f15:15::27 NIST, Gaithersburg, Maryland All services via IPV6 time-e-g.nist.gov 129.6.15.26 NIST, Gaithersburg, Maryland All services available time-e-g.nist.gov 2610:20:6f15:15::26 NIST, Gaithersburg, Maryland All services via IPv6 time-a-wwv.nist.gov 132.163.97.1 WWV, Fort Collins, Colorado All services available time-b-wwv.nist.gov 132.163.97.2 WWV, Fort Collins, Colorado All services available time-c-wwv.nist.gov 132.163.97.3 WWV, Fort Collins, Colorado All services available time-d-wwv.nist.gov 132.163.97.4 WWV, Fort Collins, Colorado All services available time-d-wwv.nist.gov 2610:20:6f97:97::4 WWV, Fort Collins, Colorado All services via IPv6 time-e-wwv.nist.gov 132.163.97.6 WWV, Fort Collins, Colorado All services available time-e-wwv.nist.gov 2610:20:6f97:97::6 WWV, Fort Collins, Colorado new server, services via IPV6 time-a-b.nist.gov 132.163.96.1 NIST, Boulder, Colorado All services available time-b-b.nist.gov 132.163.96.2 NIST, Boulder, Colorado All services available time-c-b.nist.gov 132.163.96.3 NIST, Boulder, Colorado All services available time-d-b.nist.gov 132.163.96.4 NIST, Boulder, Colorado All services available time-d-b.nist.gov 2610:20:6f96:96::4 NIST, Boulder, Colorado All services available time-e-b.nist.gov 132.163.96.6 NIST, Boulder Colorado All services available time-e-b.nist.gov 2610:20:6f96:96::6 NIST, Boulder, Colorado All services available time.nist.gov global address for all servers Multiple locations All services available utcnist.colorado.edu 128.138.140.44 University of Colorado, Boulder All services available utcnist2.colorado.edu 128.138.141.172 University of Colorado, Boulder All services available The following servers support only authenticated NTP requests using the symmetric key encryption method that is defined in the NTP documentation. They do not respond to requests for time in the DAYTIME or TIME formats and will not accept anonymous ftp connections. You must apply to NIST for an encryption key to use these systems; they will not respond to NTP requests from users who have not registered with NIST. See the authenticated NTP description for more information. Name IP Address Location Status ntp-b.nist.gov 132.163.96.5 NIST, Boulder, Colorado Authenticated service ntp-wwv.nist.gov 132.163.97.5 NIST WWV, Fort Collins, Colorado Authenticated service ntp-c.colorado.edu 128.138.141.177 JILA, Univ. of Colorado, Boulder Authenticated service ntp-d.nist.gov 129.6.15.32 NIST, Gaithersburg, Maryland Authenticated service The following server supports only the NTP format and transmits UT1 time rather than UTC(NIST). For details about the UT1 server, please see the UT1 NTP Information page. ut1-time.colorado.edu 128.138.140.50 University of Colorado, Boulder ut1-wwv.nist.gov 132.163.97.7 NIST WWV Radio, Ft. Collins, CO