T-Server for Cisco UCM Deployment Guide

T-Servers 8.1.2

12/29/2021

Table of Contents

Supplement to T-Server for Cisco UCM Deployment Guide	**3**
Agent state change on unavailable DN	**4**
Cross-cluster supervisor monitoring	**5**
Extend and connect	**6**
TLS Support	**8**

Supplement to T-Server for Cisco UCM Deployment Guide

This supplement provides descriptions of new features introduced in T-Server for Cisco Unified Communications Manager 8.1.2 as part of the T-Server Continuous Delivery project.

The current documentation set for this T-Server can be found here.

8.1.2 Features Support

The following features are described in this supplement:

Released in Version	Feature Name	Date Released
8.1.202.35	Agent state change on unavailable DN	November 13, 2018
8.1.202.34	Cross-cluster supervisor monitoring	March 2, 2018
8.1.202.15	Extend and connect	December 22, 2016
8.1.200.06	TLS	December 24, 2013

Agent state change on unavailable DN

A call routed to an agent on an unexpectedly unavailable DN could be continuously routed to that same agent. To avoid this scenario, and to avoid further routing to that out-of-service DN, you can set the agent state to Not Ready, Walkaway, or Logged Out.

You can enable this functionality in any of three ways, in order of precedence:

- For specific calls, specify the extensions key INVALID_DEST_ACTION, with a value of notready, walkaway, or logout, in the RequestRouteCall.
- For specific agents, set the option **route-invalid-dest-action** in the Tserver section of the Annex tab of DN objects.
- For all agents, set the option **route-invalid-dest-action** in the Tserver section of the application.

route-invalid-dest-action

Valid Values: *none, notready, walkaway, logout*

Default: *none*

Effective: Immediately

When T-Server receives the error code TERR_INV_DEST_DN (177) when it tries to route a call, it takes one of these actions:

- *none:* T-Server takes no action.
- *notready:* T-Server sets the agent to NotReady.
- *walkaway:* T-Server sets the agent to NotReady with work mode Walkaway.
- *logout:* T-Server sets the agent to LoggedOut.

This option does not apply when DND is enabled.

Cross-cluster supervisor monitoring

In an environment with DNs spread across multiple Cisco clusters, supervisors and agents often reside on different clusters, controlled by different Cisco T-Servers. However, the switch does not directly support cross-cluster supervision, so T-Server uses a temporary transfer process to enable supervisor monitoring across a cluster.

CTI ports, configured as Extensions with switch-specific type 2, serve as the temporary local supervisor DNs. The T-Server client uses a CTI port to requests supervision of an agent. Once the call arrives at the agent and the monitor call is established at the CTI port, the client then immediately requests a transfer to the real supervisor, specifying the location in case the supervision is controlled by a different Cisco T-Server.

The client determines:

- which CTI port to use for each monitor request, and
- where the monitor call is single-step transferred, once established on the CTI port.

Any calls to a CTI port should be transferred immediately to avoid dropped calls.

Limitations

- Only single-step transfer is supported.
- Cross-cluster supervision is limited to silent monitoring.
- A CTI port can be used for only one call at a time.
- Only MonitorNextCall is supported, so the client must request observation for every new call.

How it works

There are three steps to transfer supervision:

1. Request and establish supervision from the CTI port, as usual:
   - Make a RequestMonitorNextCall request, specifying a CTI port as the supervisor (ThisDN).
   - The call arrives at the agent and T-Server adds the CTI port to the call, indicated by EventEstablished and EventPartyAdded.
2. Make a RequestSingleStepTransfer request to the real supervisor, specifying AttributeLocation and the extension key-value pair GCTI-REMOTE-OBSERVE=true. The extension ensures that DNRole is correct, informs the destination T-Server that the destination is a remote observer, and directs that AttributeThisDNRole is set to RoleObserver (1) accordingly.
3. Answer the call at the real supervisor. This results in an EventEstablished event on the supervisor with DNRole 10. An EventPartyAdded event is also distributed if the supervisor is local.

Extend and connect

The Cisco UCM *extend and connect* feature enables an agent to use a remote phone, such as a mobile phone, to connect to the CUCM. The feature associates a remote number with a special CiscoRemoteTerminal number in the switch. This terminal essentially acts as the agent's terminal but calls end up at the remote number (remote destination) instead. Calls can be both made from and received by this remote number.

Calls made to the remote terminal can be answered through a CTI request on the remote terminal, or manually on the remote destination. Calls made from the remote terminal can be made only through CTI on the remote terminal.

This topic covers only T-Server support for extend and connect. For details, see the Extend and Connect chapter of the *Cisco Unified Communications Manager Features and Services Guide*.

Service state

All remote terminals remain out of service until both are:

- Indicated to be in service by JTAPI, and
- Successfully extended to a remote destination.

An EventDNBackInService is generated when both of these become true and an EventDNOutOfService occurs when either become false. Calls made to remote terminals that are not extended to a remote destination result in destination busy from the switch.

Activation and deactivation

To activate extend and connect on a remote destination from a remote terminal, a T-Server client performs a RequestRegisterAddress on the remote terminal address with the extension REMOTE_DEST and REMOTE_NAME set to the desired remote destination number and name, respectively. Only REMOTE_DEST is required, as T-Server uses REMOTE_DEST for both if REMOTE_NAME is not provided. The client receives an EventRegistered immediately. An EventDNBackInService is distributed with REMOTE_DEST and REMOTE_NAME extensions if the extend and connect is successful. An EventHardwareError is generated if an error occurs.

To deactivate extend and connect, a T-Server client performs a RequestUnregisterAddress or simply disconnects, causing an EventUnregistered and an EventDNOutOfService on the remote terminal.

Multiple Clients

If multiple clients request extend and connect on the same remote terminal, the last one determines the remote destination. Only this client can deactivate the extend and connect by either RequestUnregisterAddress or client disconnection, in which case all remaining clients receive an EventDNOutOfService. Clients can use REMOTE_DEST and REMOTE_NAME extensions in EventDNBackInService to determine if they have control.

High Availability

The switch notifies both primary and backup servers of extend and connect connectivity. However, synchronization is needed from primary to backup:

- In cases where a backup starts after extend and connect is already established in the primary, and
- To inform the backup of which client has control of extend and connect for a specific remote terminal.

This communication is accomplished through the primary-to-backup synchronization connection, enabling T-Server to ensure that extend and connect to remote destinations is maintained upon switchover. A switchover results in the remote terminal temporarily going out of service while the newly promoted T-Server reconnects the remote destination. The client receives an EventDNOutOfService followed by an EventDNBackInService with remote extensions.

Limitations

T-Server support for extend and connect has these limitations:

- A call to a remote terminal can be answered only manually at the remote destination. RequestAnswerCall is not supported at the remote terminal.
- Originating a call or consult from a remote terminal must be done through a CTI request. Manual origination is not supported.
- When making calls from a remote terminal, setting the delay-dialing option to `true` does not produce the desired effect of providing the dialed digits in the AttributeDNIS and AttributeOtherDN of EventDialing.

Configuration

To configure T-Server for extend and connect, configure the switch with CiscoRemoteTerminal addresses, one for each active agent. Configure each remote terminal as an Extension in Configuration Server.

TLS Support

CTI-level communication between T-Server and the Genesys Java Telephony API (JTAPI) process and the Cisco CTIManager can now be encrypted. Communication between T-Server and the Cisco CTIManager can traverse multiple network paths. Each link within T-Server communicates over a TCP connection to a Genesys JTAPI process and each JTAPI process communicates over a TCP connection to the Cisco CTIManager. Because T-Server for Cisco UCM supports multiple links, the number of network paths (CTI/TCP connections) is twice that of the number of links (2 links - 4 TCP connections, 3 links - 6 TCP connections).

This feature enables secure communication over TCP sockets originating and terminating between the JTAPI process and the Cisco CTIManager. JTAPI provides the necessary functionality required to provide two-way authentication and secure communication between JTAPI and Cisco CTIManager. This functionality is dependent on client server certificates, and is out of scope of this document.

Securing communication with JTAPI

Securing communication with JTAPI requires communication to:

1. Cisco TFTP server to obtain the trusted server certificate (using the `tls-tftp-host` and `tls-tftp-port` configuration options).
2. Cisco CAPF server to obtain the client certificates (using the `tls-capf-host` and `tls-capf-port` configuration options).

When T-Server starts, all required certificates are automatically downloaded by the Genesys JTAPI process and stored in the local folder specified by the `tls-cert-path` configuration option. These downloaded certificates are encrypted based on the password defined by the `password` option.

Each connection/link between JTAPI and CTIManager requires its own unique client certificate. To obtain a client certificate for a particular link, an authorization code and an instance ID are required. Two link-level options, `tls-auth-code` and `tls-instance-id`, represent the authorization code and the instance ID, respectively, for TLS-enabled configurations.

The authorization code is required only for the initial download of the client certificates.

The instance ID provides a method to associate a specific certificate with a specific link and is configured in the Cisco UCM database. There is a one-to-one relationship between a link and an instance ID. Using the same instance ID on different links simultaneously might cause the certificate to be invalidated by Cisco.

Note: The first initial download of the server certificate is considered trusted. For this reason, it is recommended that the initial T-Server run, after configuring TLS, be done in a secure network (environment).

Feature Configuration

To enable TLS communication:

1. Obtain the certificates.

1. Configure the following options in the **`link-tls`** section:
   - `password`
   - `tls-cert-path`
   - `tls-capf-host`
   - `tls-capf-port`
   - `tls-tftp-host`
   - `tls-tftp-port`
2. Configure the following options in the link section specified by the **`link-`*`n`*`-name`** option:
   - `tls-auth-code`
   - `tls-instance-id`
3. Start T-Server.
4. Check that certificates were obtained and are located in the directory specified in `tls-cert-path`.
5. Stop T-Server.
6. Remove the `tls-auth-code` option from the link section.

2. Run T-Server with the secure connection.

1. Ensure that the link section contains only the TLS-related option `tls-instance-id`.
2. Start T-Server.

To disable TLS communication, remove one or more of the mandatory TLS options.

Configuration Options

password

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid characters
Changes Take Effect: After restart

Specifies a passphrase used to encrypt the local key store for certificates.

tls-cert-path

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid local path

Changes Take Effect: After restart

Specifies the local directory path where certificates should be installed.

tls-capf-host

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid address
Changes Take Effect: After restart

Specifies the hostname or IP address of the Cisco UCM CAPF server. Defined by switch configuration.

tls-capf-port

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid port
Changes Take Effect: After restart

Specifies the port number on which the CAPF server is running. Defined by switch configuration (typically defaults to 3804).

tls-tftp-host

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid characters
Changes Take Effect: After restart

Specifies the hostname or IP address of the Cisco UCM TFTP server.

tls-tftp-port

Section: `link-tls`
Default Value: NULL
Valid Values: Any valid port
Changes Take Effect: After restart

Specifies the port number on which the TFTP server is running. Defined by switch configuration (typically defaults to 69).

tls-instance-id

Section: Specified by `link-<n>-name`
Default Value: NULL
Valid Values: Any valid characters
Changes Take Effect: Immediately – changing this option will cause the link to drop and reconnect

Specifies the application instance ID, as configured on the switch side (Cisco UCM). Each TLS link requires a unique ID.

tls-auth-code

Section: Specified by `link-<n>-name`
Default Value: NULL
Valid Values: Any valid characters
Changes Take Effect: Immediately – changing this option will cause the link to drop and reconnect

Specifies the authorization string configured in Cisco UCM. This code is used only once for client certificate download.