Solace Monitoring Dashboard: Bridge

Dashboard "Solace bridges" lists details on one particular messaging bridges of one broker instance and one vpn.

Details on messaging bridges can be found at https://docs.solace.com/Overviews/Message-VPN-Bridges-Overview.htm

A Solace message bridge directly connects two vpn with each other for direct exchange of messages. This exchange is configured on topics and can be configured either uni- or bidirectional.

The drop downs on top allow for selection of broker instance, the vpn and the bridge to be monitored. Selecting on one dropbox will automatically influence the list of available entries to it's right.

Bridges are configured between vpn of two Solace broker instances (Remote bridge) or between two vpn on the same Solace broker instance (Local bridge).

Bridges are monitored on each vpn endpoint individually.

Metric	Possible Values	Description	Typical Actions
Operational State	Up (green) Down (right) with history	General operational state of a bridge (On/Off switch).	A bridge should always be operational up, unless for planned maintainance or downtime. The availability of a bridge can be checked here. A bridge may be manually disconnected, however, the disconnected bridge immediately attempts to reconnect. For a longer planned downtime the bridge should be shut down.
Connection up time	time value	time since when this bridge is up and both vpn parties connected over it.	A shorter than expected value would indicate a failover event or other network interruption to have happend.
Connection establisher	auto Local Remote NotApplicable	The current configuration setting on which side should initiate the bridge connection. Local: This currently watched side of the bridge performs the initial connection to the other. Remote: The other side of the bridge performs the initial connection to this currently watched endpoint. Auto: best of both	This setting may be relevant in network restricted scenario or on more fine grained control of availability of a bridge. E.g. when a firewall would allow uni-directinal communication only between two vpn.
Redundancy	auto primary backup NotApplicable	When remote bridging to a redunadant vpn, indicates which status of the connected broker instance is targeted, in terms of redundancy. https://docs.solace.com/Configuring-and-Managing/Monitoring-Message-VPN-Bridges.htm	An appropriate configuration is highly dependant on the application architecture. An outline of typical scenario is provided at https://docs.solace.com/Configuring-and-Managing/VPN-Bridging-to-Remote-Appliances.htm

Metric	Possible Values	Description	Typical Actions
Inbound Operational Failure Reason	textual	In case of failure, an indicator is provided on the reason of failure. An indicator may be one out of: "(no failure)" "Bridge disabled" "No remote message-vpns configured" "SMF service is disabled" "Msg Backbone is disabled" "Local message-vpn is disabled" "Active-Standby Role Mismatch" "Invalid Active-Standby Role" "Redundancy Disabled" "Not active" "Replication standby" "Remote message-vpns disabled" "Enforce-trusted-common-name but empty trust-common-name list" "SSL transport used but cipher-suite list is empty" "Authentication Scheme is Client-Certificate but no certificate is configured" "Client-Certificate Authentication Scheme used but not all Remote Message VPNs use SSL" "Basic Authentication Scheme used but Basic Client Username not configured" "Cluster Down" "Cluster Link Down"	The reason code may support finding the source of issue when bridge connection fails. A primer to Solace vpn bridging can be found at https://solace.com/blog/bridging-solace-message-vpns/ . Details on the individual code is found at https://docs.solace.com/Configuring-and-Managing/Monitoring-Message-VPN-Bridges.htm#monitor_vpn_bridges inside "Example 2 – show bridge detail" in the tables on reported operational states.
Inbound/Outbound operational state	textual	Inbound/Outbund provide an overview on the availability of the bridges in and out channels. Possible indicators are: "init" - The connection is initializing. "disabled" - The connection is disabled by configuration. "enabled" - The connection is enabled by configuration. "prepare" - The connection is operationally down. "prepare-wait-to-connect" - The connection is waiting to connect. "prepare-fetching-dns" - The domain name of the destination node is being resolved. "not-ready" - The connection is operationally down. "not-ready-connecting" - The connection is trying to connect. "not-ready-handshaking" - The connection is handshaking. "not-ready-wait-next" - The connection failed to connect and is waiting to retry. "not-ready-wait-reuse" - The connection is closing in order to reuse an existing connection. "not-ready-wait-bridge-version-mismatch" - The connection is closing because of a version mismatch. "not-ready-wait-cleanup" - The connection is closed and cleaning up. "ready" - The connection is operationally up. "ready-subscribing" - The connection is up and synchronizing subscriptions. "ready-in-sync" - The connection is up and subscriptions are synchronized.	A healthy bridge connection would list • Inbound state as "Ready-InSync". • Outbound state depending of uni- or bi directional setup as "NotApplicable" or "Ready" Details on the individual code is found at https://docs.solace.com/Configuring-and-Managing/Monitoring-Message-VPN-Bridges.htm inside "Example 2 – show bridge detail" in the tables on reported operational states
Queue Operational State	Bound (green) Unbound(yellow) Unknown (red) Not Applicable	Monitor connectivity on queue over a bridge. Queue connectivity is a requirement for guaranteed message delivery across bridges.	Guaranteed messages may traverse a message vpn bridge from a remote message vpn to a local message vpn to fulfill matching topic subscriptions. However, if you want to ensure that the delivery mode of the messages delivered to the local message vpn is not changed to direct to fulfill matching client topic subscriptions on the local message vpn, queues must be used at both ends of the message vpn bridge. That is, the guaranteed messages must be delivered from a queue assigned an appropriate topic subscription on the remote message vpn to another queue assigned a matching topic subscription on the local message vpn. If the bridge doesn't start or end with a queue, Guaranteed messages with a non-persistent delivery mode can be changed to direct to fulfill matching client topic subscriptions on the local message vpn. No warnings or errors are provided when changes to messages' delivery modes occur. https://docs.solace.com/Overviews/Message-VPN-Bridges-Overview.htm#working_with_bridges_GD_msging https://docs.solace.com/Overviews/Message-VPN-Bridges-Overview.htm#working_with_bridges_avoid_loss

Metric	Possible Values	Description	Typical Actions
Subscriptions / Slow Subscriber	graphs over time	Left scale graph lists the count of remote topic subscriptions currently active. Right scale graph shows an on/off indicator whether this vpn is a slow subscriber on that bridge.	
Transfer Messages	graphs over time	The number of messages being transfered over the bridge, seperately listed for ingress (received) and egress (sent) messages, by count.	
Transfer Volume	graphs over time	The volume of data being transfered over the bridge, seperately listed for ingress (received) and egress (sent) messages, by data volume.	
Message Discards	graphs over time	The number of messages being discarded on either ingress or egress	Messages may be discarded by the broker for a variety of reasons. If those messages will be canceled in either ingress or egress, the count will apear here. Possible reasons for discards are (detailed statistic on any would be available from Prometheus data storage): Ingress: • No matching subscription • Parse error on topic • generic parse error • Message being too big to handle • Time to life (TTL) has been exceeded • Web Parse Error (REST messages) • Access Control List violation on publish • Message spool being exhausted (spool full) • Message Promotion Congestion (slow consumer) • Message Spool congestion (slow spool) Egress: • Transmit Congestion (network saturation) • Comression Congestion (cpu saturation) • Message Elided (expiry) • Payload can not be formatted (protocol capability mismatch) • Message Promotion Congestion • Message Spool Congestion • Client not connected