

# Questionnaire: Deploying in a Dedicated Cluster

This questionnaire is specific to deployments of Solace Cloud in Dedicated Clusters. For questions related to deployments in Customer-Controlled Clusters, see [Questionnaire: Deploying in a Customer-Controlled Cluster](#).

Deploying Solace Cloud can require planning and coordination across different teams. It's important that you plan and design your deployment to ensure the long-term success of your system. The following questions are designed to uncover the configuration information needed to create your event broker services properly. To help make your deployment go quickly and smoothly, carefully research and plan your decisions around these questions.

Configuration Question	How Solace Uses This Information	Related Documentation
What cloud provider do you want Solace to use?	Dedicated Cluster deployments of Solace Cloud support the following implementations of Kubernetes: <ul style="list-style-type: none"><li>• Amazon Elastic Kubernetes Service (EKS)</li><li>• Azure Kubernetes Service (AKS)</li><li>• Google Kubernetes Engine (GKE)</li></ul>	<a href="#">Deployment Architecture for Kubernetes</a>  <a href="#">Mission Control Agent</a>  <a href="#">Deployment Options</a>
In what region do you want to create event broker services?	To correctly install and configure your Dedicated Cluster deployment, Solace needs to know which cloud provider	<a href="#">Creating Event Broker Services</a>

Configuration Question	How Solace Uses This Information	Related Documentation
	region (if applicable) to use.	
<p>Do you want the Messaging Connectivity to or from your event broker services to go through the public internet, private networks, or both?</p>	<p>To help you configure the Messaging Connectivity for your Dedicated Cluster, Solace must know how you want your Messaging Connectivity routed.</p>	<p><a href="#">Solace Cloud Connectivity Requirements</a></p>
<p>Do you want your incoming Messaging Connectivity to be private?</p> <p>If so which of the networking options supported by Solace do you want to use?</p>	<p>Solace uses this information to help guide you in configuring the networking option you choose.</p>	<p><a href="#">Networking Options for Dedicated Cluster Deployments</a></p>
<p>If you want your Messaging Connectivity to be private?</p> <p>Does your chosen networking option require a unique CIDR range?</p> <p>If so, you can you an appropriately sized CIDR that is com-</p>	<p>Solace requires the CIDR to provision the VPC/VNet.</p> <p>If the network option you chose requires a unique CIDR range, you must provide one that does not overlap with any networks your event broker services will peer with. It must accommodate your network plan, and the amount event broker services you want to deploy.</p>	<p>For EKS and AKS, use the <a href="#">Excel-based CIDR calculator</a></p> <p>For GKE, see <a href="#">Networking in Installing in Google Kubernetes Engine</a></p>

Configuration Question	How Solace Uses This Information	Related Documentation
<p>patible with your network plan?</p>	<div data-bbox="552 279 1112 661" style="border: 1px solid #0070C0; padding: 10px; margin-bottom: 10px;"> <p>Dedicated Cluster customers deploying to Azure should use the <b>Azure (AKS) - Kubenet</b> page in the CIDR calculator when determining their required CIDR range.</p> </div> <div data-bbox="552 693 1112 976" style="border: 1px solid #D9534F; padding: 10px;"> <p>Consider the size of your cluster’s network carefully, as it is not possible to change its size after creation.</p> </div>	
<p>Do you want to use a self-managed key for encrypting the data at rest on the persistent storage of your event broker services?</p>	<div data-bbox="552 1016 1112 1299" style="border: 1px solid #0070C0; padding: 10px; margin-bottom: 10px;"> <p>Solace encrypts all data at rest by default. Using a self-managed key for encrypting data at rest is optional.</p> </div> <p>If you want to use a self-managed key for encrypting your data at rest you must provide the key to Solace. Self-managed keys provide enhanced security by providing you with control over the creation, management, and permissions of the encryption keys.</p> <p>Solace currently supports self-managed keys from the following providers:</p>	<p><u><a href="#">Data at Rest</a></u></p>

Configuration Question	How Solace Uses This Information	Related Documentation
	<ul style="list-style-type: none"> <li>• AWS Key Management</li> <li>• Service Azure Key Vault</li> <li>• Google Cloud Key Management</li> </ul>	

## Contact Information

You must provide a point of contact for each entry in the table below. Solace prefers a distribution list as the point of contact, though you can choose to provide individual contact details.

Contact Type	Distribution List or Contact Details
Event broker service incidents or issues.	
Event broker service upgrade notifications and scheduling.	
Release and maintenance notifications.	