

Extreme CloudOps for ExtremeCloud Edge

Service: Extreme CloudOps Service

Version: 0.03

Date: July 2023

Availability: Global

Order Code: XIQ-EDGEOPS-S-EW

Service Overview

ExtremeCloud Operations (CloudOps) provides orchestration of containerized applications onto a customer premises hosted from an ExtremeCloud Edge service. The customer is responsible for the setup of the installation and on-boarding of the ExtremeCloud Edge cluster to an ExtremeCloud IQ Account for visibility of the state of the hosting environment. Once on-boarded, Extreme's CloudOps service provides application installation, upgrade, and monitoring of the state of the application components. The application and hosting cluster is monitored 24/7 for any operational issues.

Extreme CloudOps provides and manages software upgrades of the application on a regular cadence. Daily backup of application data is also available providing protection for disaster recovery.

Service Levels

Not applicable

Availability

ExtremeCloud Ops service (CloudOps) is orderable as Bill-of. Consult the Extreme Networks Price List for listing subscription part numbers. ExtremeCloud CloudOps service for ExtremeCloud Edge is sold separately but it is an integral component of the ExtremeCloud Edge package that requires purchase of Professional Services (min 3 ESUs), three or more ExtremeCloud Edge appliances, on-site hardware replacement and a pre-defined application subscription investment.

Please ensure to review and agree to minimum terms and conditions requirements prior to order submission.

Pre-Requisites

Universal Compute Platform (UCP) Hardware cluster (6+ x 4120C-1) must be fully installed, network operational, and external access enabled prior to onboarding the Universal Compute Platform (UCP) cluster into XIQ or other applications for CloudOps. Customer must provide network setup and access

through any firewall in accordance with network access requirements described in the [ExtremeCloud Edge – Managed Orchestration Deployment Guide](#).

Firewall access must be granted to allow Extreme CloudOps Access to the installed Universal Compute Platform (Hardware) cluster and access to the application ports is always required (24/7). The firewall rules must allow incoming access from specific hosts to specific ports of the installed ExtremeCloud Edge cluster. Customers must onboard the Universal Compute Platform cluster via ExtremeCloud IQ and provide accurate information related to the network configuration of the system.

The firewall rules must allow specific access to specific destinations from the ExtremeCloud Edge to ExtremeCloud IQ infrastructure.

Remote access enabling connection of remote devices for testing and validation of operations. Extreme will assert proper operation of the application by remotely connecting automated test suites. These suites require access to the same services as a standard device (AP, Switch) requires when deployed remotely.

Deliverables

Extreme CloudOps Service includes:

Initial deployment of application. Once cluster is installed, configured for network access, and onboarded into ExtremeCloud IQ, Extreme CloudOps will deploy the application to the remote instance. The application is deployed by secure tunnel into the appliance(s).

Post-install validation of all application services. CloudOps will further coordinate Quality Assurance operations to perform functional assessment of the application, which may include executing suites of regression testcases to assert proper operation of the new installation. This assessment includes both assessment of the state of the installed components, assertion of connectivity of services within the cluster, and operational verification of the application functionality. Extreme will remotely assess the functional operation status of the installation.

The state of the application is remotely monitored by automated facilities.

Extreme Networks Responsibilities

Extreme CloudOps manages the delivery and state of the application and its related components, including any adjustments to deployment procedures or component configuration to ensure optimal operation state of the application on the hosts provided to customer location.

Software maintenance includes a regular cadence of updates to the installed application. These updates may relate to new application revisions or patches to issue resolution or security updates, under discretion of Extreme Networks. Extreme CloudOps will provide notification within two weeks to customers of maintenance timeslot corresponding to upcoming maintenance updates. Special consideration will be given to customer requests requiring specific black-out periods. The customer cannot, however, opt out of ALL upgrades.

Extreme CloudOps will ensure the application is properly installed and all services are properly configured on ExtremeCloud Edge hosting to meet its operational objectives.

Extreme CloudOps will remotely monitor the state of the application for component stability and resource utilization. Any inconsistencies in component or node states will be automatically detected by Extreme and corrective action inspected. CloudOps will undertake corrective action, either directly on the installed system or when necessary, contact customer and Extreme services (GTAC) to complete corrective action.

ExtremeCloud Ops will make available secure backup of installed application to a remote data-store for disaster recovery. Images will be stored independently in an Extreme networks account within a regional data center. Images will be backed up daily. In case of a disaster event, ExtremeCloud Ops will engage with GTAC services and customers to restore the latest image into a working cluster as soon as the cluster state is restored. Customer has the option to opt-out of this function, but by doing so, customer automatically opts out of disaster recovery support, whereby in case of failure, CloudOps involvement will consist of re-building a cluster to a new fresh state.

Customer Responsibilities

The customer is required to identify and prepare all network operations including IP addresses and firewall settings prior to the installation of the ExtremeCloud Edge Cluster.

Customer is required to provide and maintain the installation locale for the hardware components of *ExtremeCloud Edge (Cluster)*. Each system is to be installed in a properly cooled and ventilated area that complies with its defined operational range specified for the hardware appliances.

Customer is required to provide network connectivity from the application to internet access, including maintaining firewall rules that allow CloudOps access to orchestrate the state of installed application.

Customer must provide accessibility of the system to CloudOps enabling maintenance operations, such as software update and full-time (24h/7days) monitoring.

Customer must also provide proper network access between the application and any devices that require interaction with the application. For example, for *ExtremeCloud IQ application*, access to the managed devices including APs, Switches, and even other applications in the network that will interact with installed applications. If the managed devices are located outside of the installation intra-net, the customer must facilitate access by such devices through the firewall to the application instance.

Customer must also enable access of the application to all required operational services, not only infrastructure functions such as NTP and DNS, but direct access to the ExtremeCloud IQ infrastructure services such as Global Data Center(s), other Regional Data Center(s) and Licensing management services that may be required by the application.

The customer is responsible for usage of the actual application. Extreme CloudOps covers maintenance and monitoring of the application. Actual configuration of application operations, such as networks, device onboarding, licensing, policies, troubleshooting and non-application availability issues are the responsibility of the customer. Any issues related to the usage of the application, functionality, troubleshooting, bugs, design questions, etc. are supported through standard support procedures.

Assumptions

Customer has purchased Extreme CloudOps support as part of an ExtremeCloud Edge package subscription. Package includes all necessary starting hardware and entitlements for application orchestration.

Hardware is properly installed, network access in the network and through any applicable firewall is properly configured to ensure proper operation of the application. Firewall has also been configured to allow access of CloudOps operations through to the installed ExtremeCloud Edge cluster.

24/7 remote access to the installed system.

Exclusions

Connectivity interruptions attributed to customer's network, firewall access or ISP.

Service related to the feature/functionality of the application is not covered. CloudOps manages the state of the application, but any issues specific to feature/functionality of the application itself must be followed through appropriate service levels and engagement procedures for escalations and investigations through a qualified Extreme Partner or Extreme GTAC.

If Extreme Networks responds to a customer's request for service and the customer's claim of network malfunction is due to problems on the local network, access gateways or local service provider side of the demarcation point due to malfunctions in equipment or software other than that covered by this service, then customer will be responsible for additional charges for such response in accordance to Extreme Networks published time-and-material rates.

Extreme Networks responsibility to provide maintenance under this service description will be limited to the customer's side of the Customer Premises Equipment (CPE) residing on the Demarcation Point ("Demarcation Point" is defined as the point between facilities controlled or owned by the local carrier and those facilities controlled or owned by the customer). If Extreme Networks responds to the customer's request for service and the customer's claim of network malfunction is due to problems on the local service provider side of the Demarcation Point due to malfunctions in equipment or software other than that covered by this service, then the customer will be responsible for additional charges for such response in accordance with Extreme Networks published time-and-material rates.

Extreme Networks is not required to provide any services for problems arising out of:

- (i) Company's failure to implement all Updates issued under the Services,
- (ii) Alterations of or additions to the Products performed by parties other than Extreme.
- (iii) accident, natural disasters, terrorism, negligence, or misuse of the Products (such as, without limitation, fire, flood, water, wind, lightening or other acts of God, operation outside of environmental specifications or in a manner for which the Products were not designed);
- (iv) Interconnection of the Products with other products not supplied by Extreme, or
- (v) certain components, including but not limited to the following: spare fan trays, blank panels, cables, cable kits, rack mount kits, brackets, antennas, and consumable items.

Extreme Networks shall only be obligated to support the then-current revision of the Products and the immediately prior revision. Support for any earlier versions or for other problems not covered under the Services may be obtained at then-current rates for special technical services and on Extreme Networks then-current terms and conditions for such services, subject to acceptance by Extreme Networks.

Extreme Networks will have no liability or obligations for failure of the products to conform to published specifications resulting from the combination of the products with any third-party hardware or software not authorized in Extreme Networks published documentation or when caused by customer's inability to use the products if the products are operating substantially in accordance with published specifications.

Service availability is subject to geographical limitations, as advised by Extreme Networks upon request. Extreme Networks will have no obligation to meet the response times outlined in the Appendix A if the customer's site is outside of the geographical zone of service availability. If the customer purchases this service for locations outside Extreme Networks advised geographical limitations, Extreme Networks will be required only to use commercially reasonable efforts to provide services as soon as practical after receipt of a request from the customer.

This service does not include support and maintenance of any third-party software or hardware not provided by Extreme Networks. This service offering and any subsequent service renewals are subject to the terms and conditions of Extreme Networks Product End of Life and Support Plan End of Life policy.

New releases and upgrades for Application Software, or software releases, updates, or upgrades otherwise out-of-scope as defined herein. Unless elsewhere agreed in writing between the customer and Extreme Networks in a separate contract, this service does not include root-cause analysis, the provision of fault reports or lead- time/performance metrics.

Remote change management requests from customer that are not part of any network service restoration activity are outside of the scope of the Extreme CloudOps for ExtremeCloud Edge service. These requests are a separately charged and scheduled activity available from Extreme Networks.