

Cisco Metacloud™: Secure the Private Cloud



Overview

This document describes how security, confidentiality, and availability are maintained in Cisco Metacloud deployments. In addition, it defines the shared responsibility model, describes what that means for Cisco and our customers, and lists best practices that should be considered in an effort to establish the most secure cloud environment possible.

Refer to the [OpenStack Security Guide](#) for additional guidance and tips on how to secure OpenStack services. Cisco also recommends that you subscribe to the [OpenStack Security](#) project and the [OpenStack Security Advisories](#) for information about the latest OpenStack vulnerabilities.

Contents

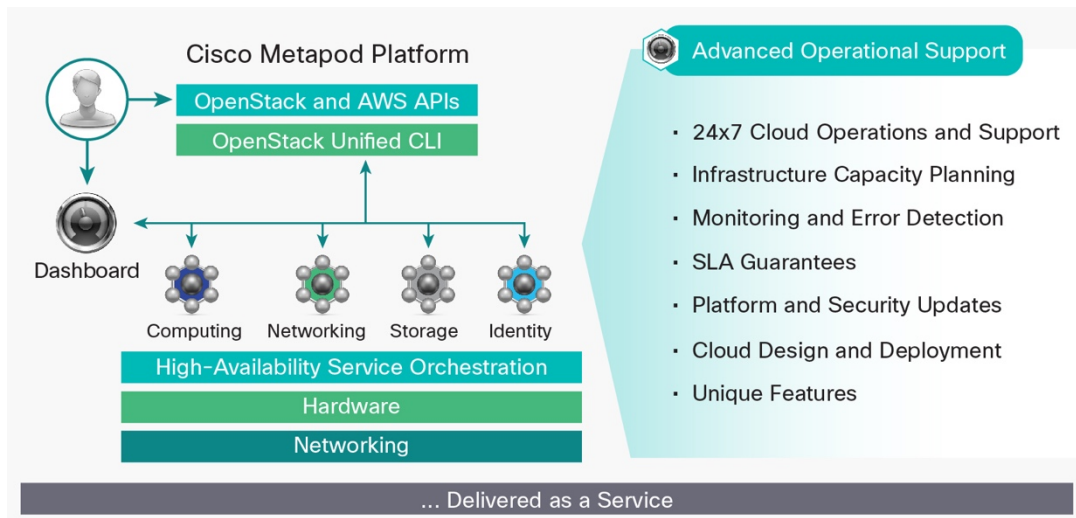
Cisco Metacloud Platform	3
Platform Architecture Overview	4
Design Requirements	6
Shared Responsibility Framework	6
Compliance Overview	7
Cisco Metacloud Security Practices	8
Network Isolation	8
Network Encryption	9
Two-Factor Authentication	9
Cisco Metacloud Corporate VPN	9
Customer-Facing VPN	10
Cisco Metadata Configuration Backup	10
Private Cloud VPN Connection	10
Dual DMZ Environments	11
Bastion Shell and Proxy Server	11
Cisco Metacloud Access and Monitoring	11
Relevant Network Protocols	12
Metadata Configuration Backup	12
Authorization and Role Management	13
Inter-Services Communications	13
Operational Security	13
Operating Guidelines for Server Configurations	13
Hypervisors	14
Secure Development Lifecycle	14
Recommended Customer Security Best Practices	15
Network	15
Storage	15
Data Encryption and Key Management	16
Data Protection and Privacy	17
Access and Authorization	17
Multitenancy	17
Node Hardening	18
API Endpoints	18
Configuration Management	18
Monitoring and Logging	19
Change Management	19
Business-Continuity Management	20
Incident Response	20
Physical Access	20
Appendix: References to Specific Certification Statements	21
Appendix: Frequently Asked Questions	25

Cisco Metacloud Platform

Metacloud is a service provided by Cisco that delivers a production-ready, OpenStack-based private cloud as a service solution. Cisco engineers deploy and operate this cloud remotely on the customer's behalf, 24 hours a day, 365 days a year (24x7x365). Figure 1 provides a summary of the platform.

More information about Metacloud can be found at Cisco Metacloud [site](#). The Metacloud service description can be found [here](#).

Figure 1. Cisco Metacloud Platform



Metacloud provides all the base components of OpenStack, including multi-tenancy, instance orchestration, user management, authentication, storage interfaces, and APIs. It also includes extensions that provide customers with enhanced fault-tolerant designs, scalability and stability features, and enterprise authentication mechanisms. The platform runs on the customer's hardware, in the customer's data center.

Metacloud helps ensure the integrity of our customers' systems by means of a multilayered security strategy. The main conceptual elements of the strategy include:

- Architectural design and delivery, based on best-practices methodologies
- Network isolation of hardened virtual private network (VPN) endpoints
- Strong encryption and multifactor authentication
- 24/7 monitoring of each environment with rigorous adherence to service-level agreement (SLA)-based performance standards

The core components of the Metacloud platform include:

- **Computing services:** Computing services provide instantiation and management of virtual machines and their associated cloud resources, including associating them with appropriate storage resources and with a project or tenant that can be accessed by appropriate users.
- **Networking service:** Networking service is a pluggable, scalable, and API-based system for managing networks and IP addresses. It provides flexible networking models to meet the needs of different applications and user groups. Standard models include both flat networks and VLANs for separation of

servers and traffic. Networking service also manages IP addresses, allowing both dedicated static IP addresses and Dynamic Host Configuration Protocol (DHCP). Floating IP addresses allow traffic to be dynamically rerouted to any computing resources, which allows traffic redirection during maintenance or in the case of failure.

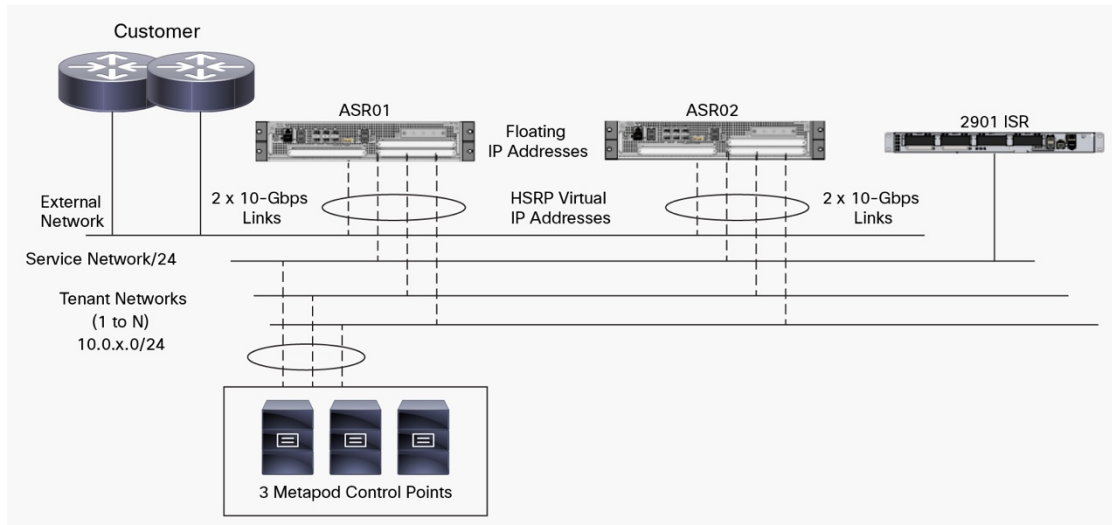
- **Storage services:** Storage services in the Cisco platform enable distributed block storage capabilities, as well as support for traditional enterprise storage technologies, such as network-attached storage (NAS). This service automates the provisioning and management of storage resources to instances, creating a complete VSAN in the private cloud environment.
- **Image service:** The image service provides discovery, registration, and delivery services for virtual machine disk and server images. It provides the capability to copy or create a snapshot of an image and immediately store it. Stored images can be used as templates to get new servers up and running quickly and more consistently than when you install a server operating system and individually configure additional services. The image service can also be used for backup purposes and includes an API and a standard representational state transfer (REST) interface.
- **Dashboard:** The Metacloud dashboard provides administrators and users with a graphical interface to access, provision, and automate cloud-based resources. The dashboard offers just one way to interact with cloud resources. Customers can automate access or build tools to manage their resources using the native OpenStack API, SDK or command line tools.
- **Identity service:** The identity service provides a central directory of users mapped to the various services that they can access. It acts as a common authentication system across the cloud operating system and can integrate with existing back-end directory services, such as Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP). It supports multiple forms of authentication, including standard username and password credentials, token-based systems, and AWS-style logins. Additionally, the service catalog provides a searchable list of all of the services deployed in the cloud in a single registry. Users and third-party tools can programmatically determine which resources they can access and how to access them.

Platform Architecture Overview

Metacloud augments the high availability of core OpenStack services (OpenStack APIs, message bus, configuration database, etc.) with unique functions to optimize continuity of services. Central components of the software design and architecture are the Metacloud control point cloud controller nodes. These control point nodes serve as the control plane and provide high-availability functions for the core components of the solution. Cisco software dynamically balances cloud service requests across all controller nodes, providing fault tolerance. In the event that one node fails, requests are transparently directed to an alternative controller.

In order to ensure that highest levels of service are delivered, Metacloud separates the control plane from the data plane. Metacloud uses the OpenStack Neutron API to delegate Layer 3 networking responsibility to two physical Cisco ASR 1000 Series Aggregation Services Routers. See Figure 2 for the architecture overview.

Figure 2. Cisco Metacloud Architecture Overview



Network Design

Neutron networking consists of several data models: router, network, subnet, and port. The Neutron router is a software router that creates an isolated network topology that has its own IP tables, Network Address Translation (NAT) rules, etc.

Each Neutron router creates an isolated network name space. In the Metacloud model, each Neutron router is represented as a virtual routing and forwarding (VRF) configuration in the physical ASR device.

A Neutron port represents a virtual switch port on a logical network switch. Virtual interfaces are attached to ports. The logical port also defines the MAC address and IP address. When an IP address is associated with a port, that port belongs to the subnet with which the IP pool is associated.

Ports are usually created when you perform the following actions:

- Boot an instance under a subnet
- Assign a floating IP address to an instance
- Attach an internal network interface to a Neutron router
- Set a gateway to a Neutron router

A Neutron network is a container of Neutron subnets and ports and is either shared or non-shared. Shared networks can be used by any tenant, whereas non-shared networks are visible only to their tenants. Networks are also flagged either public or private. A public network is an external network while a private network is internal. Only an administrator user can operate on an external network. In the Metacloud network architecture, only one external network can be used.

A Neutron subnet represents an IP address block that can be used to assign IP addresses to virtual interfaces (fixed and floating IP addresses). Each subnet is defined by classless interdomain routing (CIDR), the VLAN ID, and the network to which it belongs. For Metacloud's Neutron network, only the VLAN subnet is supported.

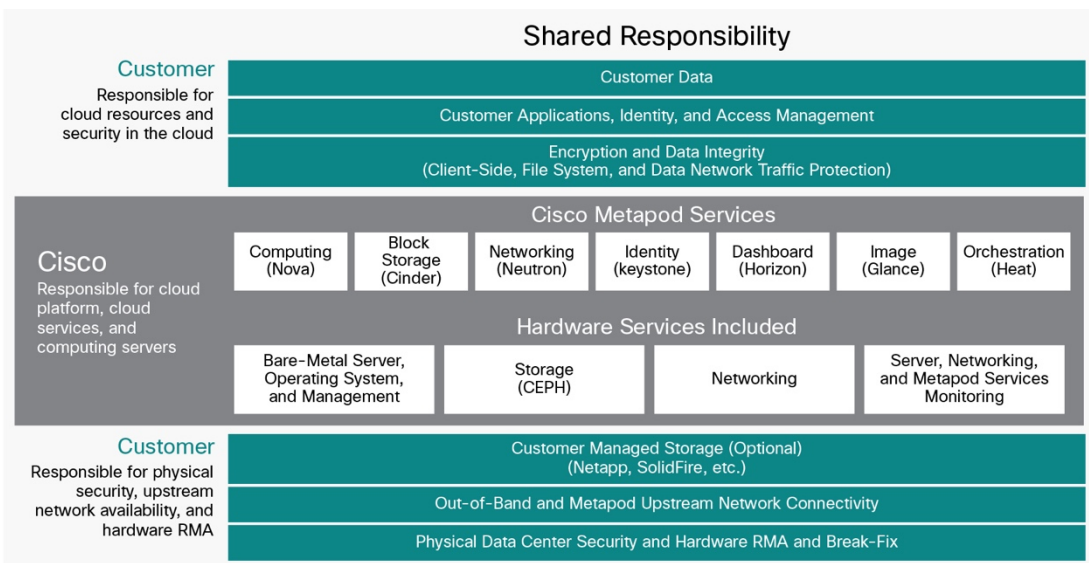
Design Requirements

A [design and installation guide](#) is available to further explain Metacloud system design, installation and configuration. The latest version of the Cisco Metacloud Controller Bundle Design and Implementation Guide can be found on the Metacloud support website at the following URL: <https://support.metacloud.com/entries/95982978-Controller-Bundle-Installation-Guide>.

Shared Responsibility Framework

Metacloud operates within a shared responsibility model, with responsibility for security shared between Cisco and its customers. The shared security responsibility framework is intended to increase customers' overall security and reduce their operational obligations by using Metacloud to supplement their existing IT infrastructure and security capabilities.

Figure 3. Shared Responsibilities



Cisco is responsible for the security of managing the OpenStack platform and uses a variety of best practices to fulfill this responsibility, such as:

- Operating System (OS) hardening using secure audit trail logging
- SSL and Transport Layer Security (TLS) encryption on API endpoints
- Restricted Cisco support access through our secure administrative gateway
- Automatic instance failover
- Automatic network range expansion

Metacloud customers are responsible for systems or hardware connected to the cloud, as well as for securing and storing customer data on their hardware in their data centers.

The sections that follow outline Cisco's and the customers' responsibilities in running a secure, trusted cloud using Metacloud.

Compliance Overview

The Metacloud architecture and infrastructure is built on security best practices. Cisco's management of the private cloud is aligned with the goal of helping our customers achieve compliance in challenging regulatory and audit environments. Using audit-friendly concepts, Metacloud provides a clear and well-defined shared responsibility framework that helps customers comply with the following IT standards and requirements:

- Service Organization Controls (SOC) 2, Statement on Standards for Attestation Engagements (SSAE) 16, and International Standard on Assurance. Engagements (ISAE) 3402
- Payment Card Industry (PCI) Data Security Standards (DSS)
- International Organization for Standardization (ISO) 27001

The appendix provides a mapping of the control domains of these standards to the security best practices described in this document.

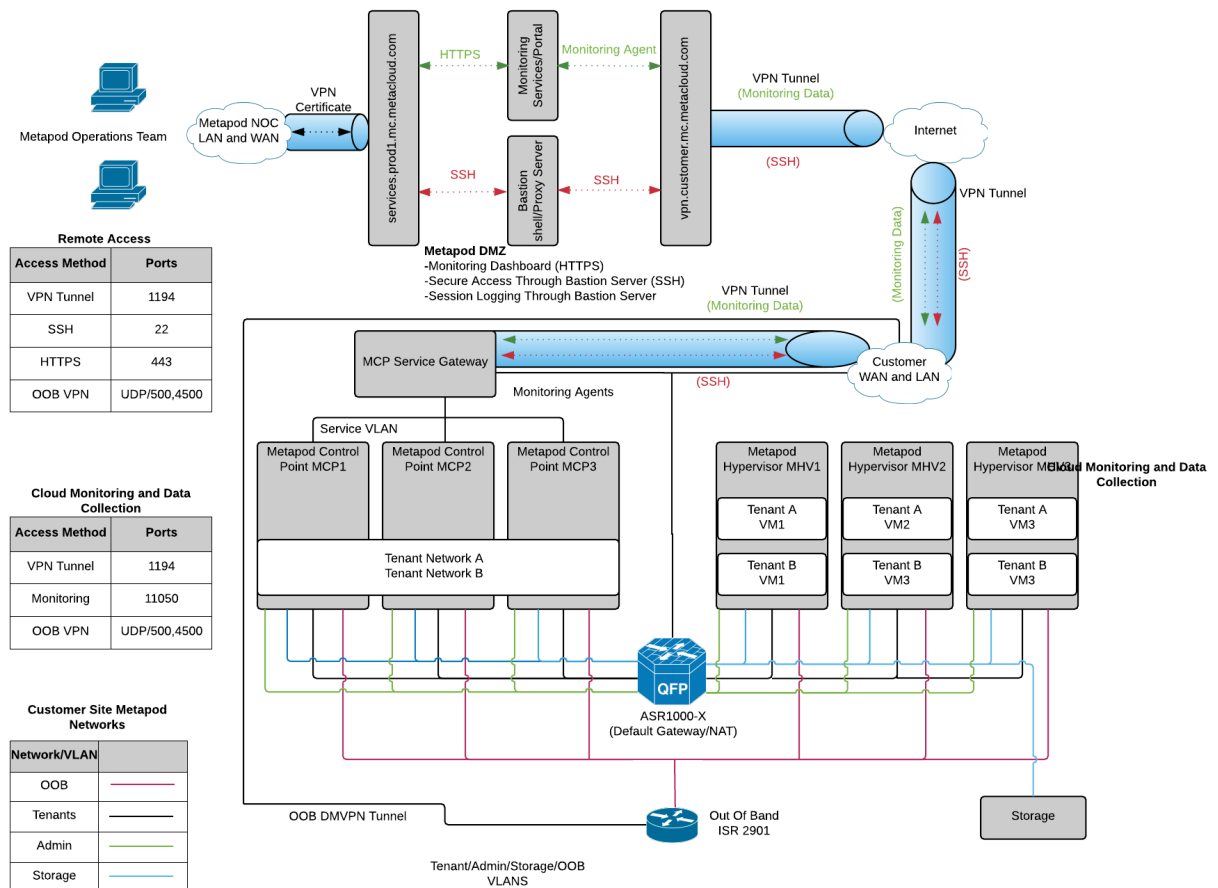
Cisco Metacloud Security Practices

Successful deployment of private cloud solutions requires a design and governance model based on shared responsibility between the customer and Metacloud.

It begins with a diligent understanding of customer security policies, existing network and data center architectures, and all relevant infrastructure operational practices. This knowledge allows each Metacloud deployment to be tailored to the specific needs of a customer's environment, based on several important security concepts.

The Cisco Metacloud team connects to the customer environment to provide 24x7 support (Advanced Operational Support) and manage the private cloud instance. Figure 4 shows a full topology, including access points, connectivity, and related management nodes (customer side and Metacloud control points).

Figure 4. Access and Monitoring



Network Isolation

The basis of our network isolation strategy is the use of dual DMZ environments: one for the Metacloud corporate VPN and a second for the customer-facing VPN. Both DMZ environments are bound by a highly controlled firewall and connected to a secure gateway network. The gateway restricts the passage of any traffic, other than authenticated and audited protocols, to the customer-facing VPN.

In addition, both the Metacloud corporate VPN and the customer-facing VPN operate within a hardened and efficient (reduced footprint) Linux-based system. External access to the VPN is limited to a single exposed port (VPN protocol) and remote network sessions (Secure Shell [SSH]) are not allowed.

Network Encryption

Our multi-tiered encryption is enforced at all critical connection points: the administrator's connection to the Metacloud corporate VPN is authenticated by means of a 2048-bit encrypted certificate (unique to the administrator) and further validated by two-factor authentication (using Google Authenticator) for the administrator's device. After this connection has been authorized, access then requires the administrator's personal SSH key, again encrypted (2048-bit strength).

Two-Factor Authentication

Metacloud uses a Bastion server to provide an additional layer of security for authentication and access control. Access to the Bastion servers is allowed only by means of the Metacloud corporate VPN. The VPN itself is a hardened Linux system with no ports exposed other than those dedicated to VPN protocols.

The OpenVPN server requires both a certificate and two-factor authentication to connect. That certificate and the SSH keys held by the administrator are encrypted, as described in the previous section, and are not shared for any other purposes.

After the user is connected to this VPN, access is further restricted through IP address tables (provided by the Linux kernel firewall) and allows only SSH access to the Metacloud Bastion server and HTTPS access to the Metacloud monitoring system. No other ports or protocols are allowed. This approach prevents passage of any unintentional traffic (from the administrator's office or remote network).

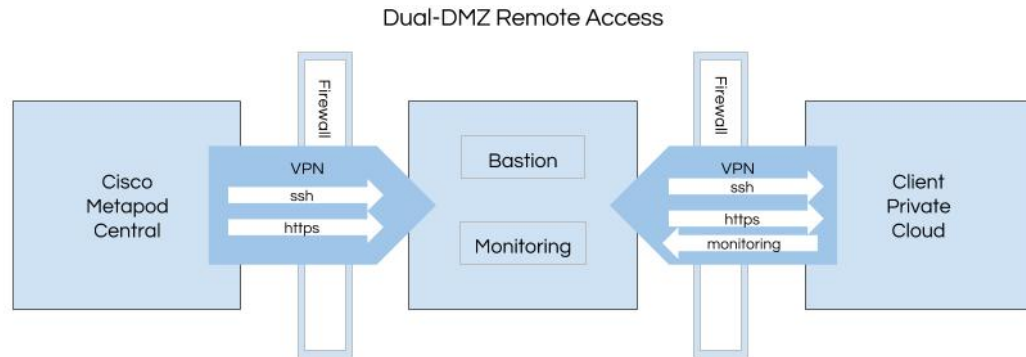
These measures help ensure the integrity of all customer resources while providing Metacloud management with a central and secure point for monitoring, administering, auditing, and (in situations requiring such action) revoking credentials.

Cisco Metacloud Corporate VPN

To perform routine maintenance and troubleshoot any system problems as they occur, the Metacloud operations staff connects to the customer's administrative VLAN through the Metacloud corporate VPN from the staff's desktop systems, as shown in Figure 5.

No special privileges are granted to the Metacloud office network or to anyone traversing that network. Thus, any communication with customer sites requires an authorized connection to this VPN. Additionally, the administrator's system does not have direct Layer 3 access to the customer network. This VPN connection allows administrators to make SSH connections only through the Metacloud SSH (Bastion) proxy gateway.

Figure 5. Cisco Metacloud Central Management Infrastructure Environment



These bounded privileges help ensure that all connections to customer networks are authenticated and auditable. They also protect customers from any direct exposure to the administrator’s local network by introducing an “air gap” (additional isolation) between systems, with firewall scrutiny and packet inspection between each clarified segment.

Customer-Facing VPN

Each customer has control nodes called Metacloud control points or cloud controller nodes. The Metacloud control points implement a “dial home through VPN” feature for Metacloud administrative access and monitoring of the cloud. As with the Metacloud corporate VPN, this VPN connects to a hardened VPN server, and the connection is authenticated using a 2048-bit certificate unique to each customer.

Cisco Metadata Configuration Backup

After connection, the hardened VPN allows only traffic from systems located in the Metacloud central management segment, through a small subset of ports. The Metacloud central management segment is a secure network isolated by VPNs located within the DMZ, between the secure network and the Internet. As previously documented, the customer-facing VPN server exposes only the VPN protocol ports to remote networks; all non-required protocols are restricted due to the hardened Linux system that governs their operation.

Private Cloud VPN Connection

During the installation process, the Metacloud control points are connected to a remote Metacloud VPN service (as an access and monitoring gateway), allowing the Metacloud operations team to monitor, maintain, manage, and, when necessary, troubleshoot the cloud services. Figure 6 shows a standard customer VPN network.

Figure 6. Customer VPN

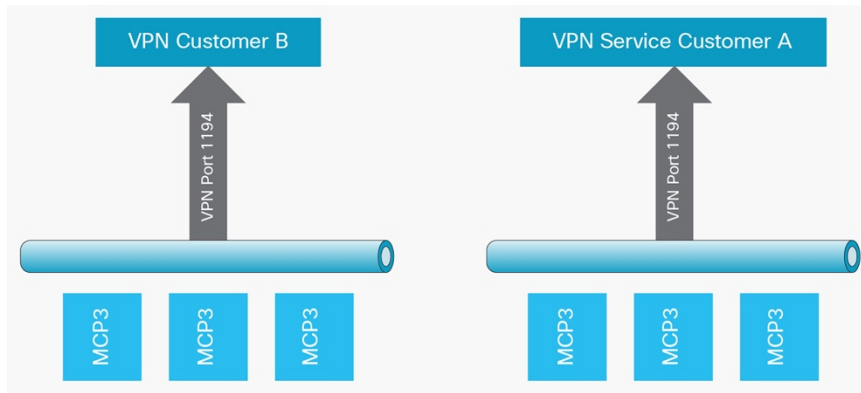


Table 1. Customer VPN Access Method and Port

Access Method	Port
VPN	1194

Dual DMZ Environments

The Metacloud DMZ schema, as illustrated in Figure 4 earlier in this document, includes the Bastion shell and proxy server and also the Metacloud central monitoring service.

Bastion Shell and Proxy Server

Metacloud's SSH Bastion server provides an additional layer of security for authentication and access logging. It is accessed through a secure connection either by SSH or HTTPS.

The gateway is located in a secure network segment that is not directly attached to the public Internet, Metacloud office networks, or customer administrator networks. This gateway exists between a pair of hardened firewalls that allow only specifically documented traffic between the VPN-connected endpoints.

As previously stated, the Metacloud SSH Bastion server is a hardened Linux system.

Connections to the SSH Bastion server are protected at Layer 3 by the VPN servers and firewalls that provide access to the secure network in which it resides. The restricted rules governing the SSH Bastion server allow connections only from the administrator's VPN segment on the SSH protocol port (port 22, using TCP).

The only port exposed on this system is SSH, which is protected by requiring use of each administrator's personal SSH key with at least 2048-bit strength.

Table 2. Administrator Access Method and Port

Access Method	Port
SSH	22

Cisco Metacloud Access and Monitoring

Metacloud, using standard monitoring tools, gathers and analyzes metrics for more than 70 critical functions in the customer environment. All cloud services are monitored, in addition to many fundamental operational categories (maximum CPU utilization, maximum memory utilization, maximum storage utilization, etc.). Monitoring is

performed 24x7x365. All events are logged and reviewed with Metacloud proactively notifying a customer when an event has occurred, per the Metacloud service level agreement with the customer.

Table 3 lists the only ports exposed for monitoring the cloud environment.

Table 3. Ports Exposed to Monitor the Cloud Environment

Access Method	Port
SSH	22
HTTPS	443
Agent	10050

Relevant Network Protocols

Except for the network protocols and ports identified here, the Metacloud network by default prohibits all network protocols, both ingress and egress.

- VPN nodes: The VPN nodes allow only port 1194 (TCP and User Datagram Protocol [UDP]) used by OpenVPN from remote networks. All other traffic is disallowed.
- SSH proxy gateway: The SSH proxy gateway allows only SSH port 22 (TCP) from remote networks.

Note: This system disallows IPv4 forwarding and does not perform any traffic routing.

- Metacloud control point nodes (cloud controller nodes): The Metacloud control point nodes allow only remote network connections through the VPN tunnel. The VPN tunnel traffic is restricted to allow SSH port 22 (TCP) from the Metacloud SSH gateway. It also allows Zabbix protocol port 10050, which is used by the Metacloud monitoring system, as well as ICMP echo requests for basic VPN connectivity validation.
- Metacloud hypervisor nodes (Cisco hypervisor nodes): The Metacloud hypervisor nodes allow only remote network connections from hosts located on the local administrator segment, as well as SSH connections routed through the Metacloud control point nodes over the secure tunnel and initiated by the Metacloud SSH gateway located in the secure network segment.
- IP address table rules: Each system in the Metacloud environment has highly restricted and deliberate IP address table rules that allow only necessary ports and protocols to be established. The default policies on all systems are defined to drop all traffic from input and forwarding, and only specifically defined traffic is allowed, as noted earlier.
- Out-of-band (OOB) access: OOB access is used only to reach the console or management ports on the Metacloud control point nodes. Cisco uses a Cisco 2901 Integrated Services Router (ISR) to provide OOB access to all the servers and networking components of the Metacloud controller bundle. This connection provides remote console connectivity for Metacloud operations. The 2901 ISR requires an initial one-time configuration and initial bootstrap process. All future maintenance and upgrade operations are performed remotely by the Metacloud operations center as part of operating the service.

Metadata Configuration Backup

Metacloud backs up some configuration metadata for support if problems arise. Data is encrypted prior to being moved offsite. Metacloud does not back up customer data or data internal to virtual machines, including both memory and storage. Metadata stored by an OpenStack cloud includes the following items:

-
- Configuration files, including OpenStack, operating system, firewalls, and IP tables (these files contain host names and IP addresses)
 - OpenStack database files that contain IP addresses, user accounts, host names, and associated metadata

Authorization and Role Management

The Metacloud platform uses preconfigured roles and assignments for all administrators, helping ensure that these roles provide fine-grained authorization for specific actions and are defined to meet typical compliance or operational needs.

Inter-Services Communications

All communication between Metacloud services is performed using REST API calls. All external API endpoints used by the Metacloud management infrastructure are secured through SSL/TLS. All API endpoints reside on a dedicated 802.1Q VLAN and are protected via a firewall. All API calls use a key management system, as part of OpenStack, to enforce signed, authorized API calls. API endpoints are protected from being flooded with API traffic by the use of usage quotas and throttling mechanisms, as provided by OpenStack. This configuration is consistent with the general OpenStack platform standards.

Operational Security

Cisco's operational policies and procedures set a high standard for each employee directly participating in the support of a customer's cloud environment. These corporate standards cover critical functions such as:

- Strong authentication mechanisms
- Dual-factor authentication
- Password length and complexity rules
- Badged access
- Automatic workstation locking
- Documented change-management and escalation procedures
- New-employee training
- Secure VPN-based access
- Monitored and auditable access

Cisco maintains documented operational procedures for all interactions with infrastructure and customer support. Newly provisioned infrastructure undergoes appropriate testing procedures to limit exposure to any hardware failure. Documented procedures and configuration version controls provide protection from errors during configuration. Changes to an existing infrastructure are controlled by a technical change-management policy that enforces best-practice change-management controls, including impact and risk assessment, customer signoff, and backout planning.

Operating Guidelines for Server Configurations

Server and operating system configurations are governed by Cisco's configuration management system. All configurations are tracked, versioned, and auditable through a version control system. All changes to configurations follow appropriate change management procedures.

The configuration guidelines for all servers and operating systems managed by Advanced Operational Support adhere to the following guidelines:

-
- Servers and operating systems are hardened, helping ensure that only packages, services, and applications required for the running of the cloud platform are enabled. All others are removed or disabled.
 - Access to servers is logged and protected through strict access-control methods.
 - The most recent security patches are installed on the servers as soon as practical and approved as part of customer change-control procedures.
 - All remote access is performed over secure channels (for example, encrypted network connections using SSH or IP Security [IPsec]).
 - All login protocols use multifactor authentication.
 - Running server configurations in customer environments are checked against stored configurations in the Cisco configuration management system on a regular basis. At the time of the check, servers are reconfigured automatically to the desired stored state.

Hypervisors

The Metacloud platform runs the Kernel-based Virtual Machine (KVM) hypervisor. KVM provides full virtualization of the Linux operating system. KVM is the leading open-source hypervisor and is trusted for its performance and security. Because KVM is built into Linux, KVM guest processes are subject to all the usual user space and process separation that is integral to the Linux kernel's operation, which has been tested and certified by numerous third parties.

Secure Development Lifecycle

Cisco supplements the scrutiny of the OpenStack development community with additional review and testing. All code and configuration changes require peer review and explicit approval. All code written by Cisco engineers includes extensive unit tests, and test coverage and successes are validated by our continuous integration process before code is accepted into a customer release.

Recommended Customer Security Best Practices

The following sections outline important security best practices that Cisco recommends customers adopt to secure their Metacloud environments, because customers are responsible for the hardware, applications, and data running in their private clouds, which can be hosted either in their own data centers or in that of third parties.

Note: These recommendations assume that the customer already has standard physical and operational security measures in place to provide comprehensive, in-depth security to protect its facilities, endpoints, networks, hosts, applications, data, users, etc. across the enterprise.

Network

Metacloud fully supports the OpenStack networking features and API to enable customers to define, use, and consume networking resources based on their requirements. This section provides a high-level overview of best practices that should be considered for implementing networking in a Metacloud cloud.

- Use the network design principles for Metacloud outlined earlier to implement VLANs, Layer 2 tunneling, subnets, IP address tables, and access control lists (ACLs) to manage network traffic in the private cloud for all your projects and tenants.
- Configure both default egress and ingress security groups at the virtual machine level to avoid unintended traffic because OpenStack default security groups allow all egress traffic even though all ingress traffic is dropped.
- Use two-factor authentication to restrict remote access and other highly privileged accounts, including network devices such as firewalls, and routers.
- Track changes to firewall ACLs using the change-management process.
- Consider the impact of encrypted traffic that may be unreadable by the intrusion detection system (IDS).
- Transmit IDS logging through the management network.
- Implement and maintain filtering rules through a central management console using Neutron services.
- Control access to the console to a specific user group of administrators and log all activity.
- Create an acceptable use policy that outlines what end users can and cannot do on the cloud network.

Storage

Metacloud backs up all the configuration data for a customer's private cloud environment in the event that it needs to be restored to a previous state for operational or emergency reasons. The customer is still responsible for managing its virtual machines, applications, and data through the complete lifecycle, including performing regular backup operations and testing recovery procedures.

Metacloud provides two options for a customer's data storage needs. The first option is to use the pre-integrated storage provided with the Metacloud infrastructure bundle. The second option is to integrate Metacloud with the customer's existing SAN or NAS storage. The storage option used depends on the customer's requirements, and the choice of storage option is beyond the scope of this document. For either storage option, Cisco recommends the following best practices:

- Develop a backup retention policy that defines backup frequency based on business needs to replicate data to different storage drives within the same availability zone to address component failures.

-
- Use a secondary availability zone to store data backups in the event of a catastrophic event where the entire primary availability zone is unavailable.
 - Monitor logs for the backup server daily to determine and resolve the root causes of problems.
 - Test data recovery procedures on a regular basis.
 - Provision access only to authenticated users and clients for the backup server.
 - Use data encryption for the storage of backups if the primary data is encrypted.
 - Enable the appropriate encryption library and select parameters to specify the algorithm and key size for all data in need of encryption using third-party tools, because Metacloud currently does not support volume encryption.
 - Verify that data volume backups are encrypted and that access is restricted through explicit authentication and authorization using Keystone services, if the primary data is encrypted as well.
 - Perform detailed logging and monitoring of all backup data being accessed.

Data Encryption and Key Management

Often customers need to encrypt their data for various business or regulatory needs. However, encryption needs to be balanced against the need to maintain satisfactory performance. A full discussion of this topic is beyond the scope of this document, but in general, Cisco recommends the following best practices if customers need to enable data encryption in their private clouds:

- Implement a third-party key management service for enhanced security using either a hardware security module (HSM) or a virtual security module (VSM) to generate, store, and rotate encryption keys, and, consider using a third-party product that protects keys in memory if sensitive data is encrypted in a virtual machine.
- Store and manage encryption keys in dedicated hosts separately from other Metacloud hosts in the environment with the highest level of access control and detailed monitoring enabled.
- Encrypt the volume data contained in Small Computer System Interface over IP (iSCSI) packets during transport to prevent snooping in a shared infrastructure being used by the private cloud.
- Consider using an encryption system with public key infrastructure (PKI) or a two-factor access control mechanism to protect sensitive data.
- Consider alternative methods to encryption, such as tokenization, when search functions need to be preserved in applications and data.
- Validate that the strength of cryptographic algorithms meets the minimum standard.
- Limit encryption keys to one process or one purpose whenever possible to limit the potential damage of key compromise.
- Store encryption keys in a purpose-built HSM or VSM.
- Assign designated custodians using the four-eyes principle to manage encryption keys.
- Develop a policy for the rotation of encryption keys.
- Log, monitor, and periodically audit access to encryption keys, limiting the number of custodians who have access to the smallest number possible.

Data Protection and Privacy

Customers with stringent compliance, regulatory, or privacy requirements often need to provide advanced data protection and privacy capabilities in their clouds. For them, Cisco recommends the following:

- Develop an inventory of information assets by the type of data contained and the relative risk in the Metacloud cloud environment.
- Apply the enterprise data retention program to meet applicable business, legal, and regulatory requirements.
- Document, track, and verify when storage media is sanitized because this data will be helpful for compliance activities (for example, meeting the European Union Data Protection Directive).

Access and Authorization

Metacloud fully supports OpenStack's various authentication and authorization features, including integration with the customer's existing Active Directory and LDAP stores. Security Assertion Markup Language (SAML)-based tokens currently are not supported to enable features such as single sign-on (SSO). Cisco recommends the following best practices for access and authentication:

- Develop access control policies consistent with the compliance, risk, and regulatory environment to cover the various user roles that will be associated with the private cloud.
- Manage identities by integrating with an external LDAP or Active Directory data store, using AuthN/Z services from Keystone. Doing so will maintain the benefits of your existing account management system with no need for duplication of workflows.
- Provision all administrator and user accounts using the principle of least privilege and explicit renewal within a period not to exceed 90 days.
- Assign each Metacloud administrator and user unique security credentials using Keystone's groups and roles functions to prevent the sharing of passwords and keys.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Require virtual machines running within Metacloud with sensitive data to enforce client-side authentication with TLS using security certificates.
- Do not use self-signed security certificates in production environments. Use only certificates issued by a certificate authority (CA).
- Track and audit all user account creation and revocation on a regular basis.
- Carefully review the expiration value of all tokens issued to users to help ensure that it does not exceed the maximum allowable time, to prevent malicious activities.
- Use encryption or tokenization to restrict access to any sensitive or confidential data (for example, cardholder data) to those with a business need to know.
- Track and monitor all access to network resources and cardholder data (if applicable).

Multitenancy

A core element of the Metacloud platform is its support for multitenancy. Project isolation is used to prevent unrestricted communication between business units or application domains. This best practice safeguards against cross-VLAN communication by restricting all ingress traffic based on destination port and source IP addresses by default.

The Metacloud solution supports industry-standard IEEE 802.1Q secured VLAN networks. For truly secure multitenancy, Cisco recommends the following best practices:

- Create an individual IEEE 802.1Q VLAN network and Layer 3 network segment for each Tenant.
- Ensure that IP address table firewalling prevents any connectivity that has not been explicitly authorized. This approach allows lower-security projects, such as a test environment, to share hardware resources with highly critical services, such as production services, without any risk of cross-contamination.

Node Hardening

The image service provided by the Metacloud platform can integrate with a customer's existing change-management and image-release processes. This integration allows the use of an organization's existing, hardened images.

The process for hardening an OS deployment or node at the virtual machine level is highly dependent on the hypervisor, virtual machine, and OS technologies being used, and we recommend customers follow those technologies' specific guidelines. As general principles, Cisco offers the following guidance for customers' consideration:

- Consider using a file integrity management (FIM) tool to prevent system or configuration files from being corrupted or changed to allow unauthorized access.
- Develop a baseline of regularly loaded or used files by using the **lsmod** command and compare that baseline to FIM checks to manage the appropriate configuration files in that environment.
- Configure file systems as read-only, to prevent writable file systems from running code.
- Implement mandatory access control policies to help ensure that user access conforms to the principle of least privilege.
- Use a host-based IDS to detect security breaches based on log analysis, policy monitoring, match of in-memory process images with on-disk executables, etc.

API Endpoints

Metacloud supports the OpenStack API to enable customers to interact with all the resources made available in the platform. If customers want to use these APIs to enable other third-party tools or applications (for example, IT services or financial management applications), they can consume these APIs. Cisco recommends the following techniques for protecting access to API endpoints in a customer's private cloud:

- Customer applications that interface with the APIs should undergo adequate security testing and follow application security best practices.
- Customers should consider tightly restricting access to API keys and certificates for account credentials to those employees and clients with legitimate business requirements. Customers should also consider segregation of duties to maintain accountability.
- Review RBAC credentials to help ensure that only authorized users can invoke Metacloud APIs.

Configuration Management

Metacloud uses a robust configuration management system to manage its cloud software. Customers are responsible for the configuration of their virtual machines. Consider the size and complexity of running a multitenant cloud environment and use the following best practices for designing a secure configuration management system:

-
- Automate builds through templates and cookbooks to help ensure consistent deployments using tools specialized for OpenStack.
 - Use a configuration management database (CMDB) to track assets and manage the overall lifecycle of the private cloud, especially if there are strict compliance or regulatory requirements in play.
 - Integrate build processes with security auditing tools.
 - Harden all configuration baselines and review them regularly for updates.
 - Restrict read and write file permissions to Keystone.conf to OpenStack service owners only.

Monitoring and Logging

Metacloud provides extensive monitoring for the components that make up a Metacloud deployment, including but not limited to servers, networking and OpenStack APIs and services. To implement security best practices, customers should also consider the following with respect to monitoring and logging of their virtual machines or instances to make their cloud environments more secure and trusted for their tenants:

- Use the OpenStack Notifier stream in security information and event management (SIEM) tools and review the history of actions and processes performed for all virtual machines.
- Monitor log sources to verify that source functions and configurations are performing as expected.
- Prioritize log entries using data fields, such as Log Source, Frequency, Time and Date, and Message Code.
- Securely store and manage logs in a central location to help facilitate analysis in the event of an incident.
- Secure archived log files using appropriate logical and physical controls, such as controls to help ensure that no one has write access to logs, and integrity controls to help ensure that no one has tampered with the logs.
- Configure logs to generate clear and actionable risk-based events that can be used during investigations.
- Use Warn mode for all logging in Metacloud production environments to prevent accidental exposure of user credentials.

Change Management

Metacloud has comprehensive change-management capabilities to manage its cloud software. The Metacloud platform is updated periodically for the latest patches and other bug fixes. Cisco notifies the customer whenever there is a significant change to the platform. Cisco recommends that customers consider the following change-management best practices for their clouds:

- Initiate the patch management process throughout the change-management process, and review the environment periodically to confirm compliance by comparing the current patch to the expected results.
- Integrate change-management processes with baseline configuration standards, so that any technology changes trigger an update of such standards.
- Continuously monitor and approve change-management processes.
- Define segregation-of-duties requirements within the change-management process and enforce them through process and technology controls to help ensure that the person requesting the change is not the same person implementing the change.

Business-Continuity Management

Cisco delivers cloud-based managed services built on a highly resilient, adaptable IT infrastructure. Cisco's business-continuity management is designed to endure system or hardware failures in Metacloud data centers while being nearly transparent to a responsive customer network. Customers are responsible for managing disaster recovery and high availability of the infrastructure, which includes external network, virtual machines, and hardware.

Cisco recommends the following security best practices for optimum business-continuity management in the private cloud:

- For redundancy, consider a secondary availability zone to maintain high availability for virtual machines.
- Create a business-continuity plan to help ensure that Metacloud cloud users can access their applications based on recovery-point objectives (RPOs) and recovery-time objectives (RTOs), and periodically test the plan and update it when major changes occur.
- Perform business impact analysis (BIA) throughout business functions, and review and track BIA results for continuous improvement.

Incident Response

Metacloud maintains an incident response plan that is proactively governed using a documented process to detect and resolve incidents all the time, every day. Metacloud SLAs are used to help determine priority, and executive leadership has visibility into the Metacloud services and receives communications for ongoing acceptance and support.

Cisco recommends that customers consider the following security best practices for incident response for their private clouds:

- Create formally documented roles and responsibilities and communicate them to staff.
- Capture detailed incident-related metrics that are regularly communicated to stakeholders and executive leaders or a formal governance body, such as an oversight committee.
- Develop scenario-based procedures for incident handling.
- Develop an incident classification that is reviewed and updated periodically.
- Identify, document, and communicate regulatory reporting requirements.
- Provide detection and response capabilities 24 hours a day, every day.

Physical Access

Metacloud uses industry-leading practices to provide physical and operational security of its data centers, which contain the Metacloud support infrastructure. These practices are certified by third parties based on standards such as ISO 27001. Customers should also consider the best practices listed here in managing the physical and operational security of their Metacloud environments:

- Create a physical access policy and procedures to define data center protection requirements.
- Restrict physical access to the Metacloud environment only to individuals with business needs.
- Add authentication mechanisms (for example, two-factor authentication or biometrics) and alarms to sensitive areas.

- Log and monitor physical access activity for all areas.
- Define the process for managing visitor access and include escort, monitoring, and logging requirements.
- Monitor compliance with the physical access process.
- Periodically evaluate physical access controls for effectiveness and update them as necessary.
- Train the appropriate facility staff in emergency procedures and the use of emergency equipment.

Appendix: References to Specific Certification Statements

Table 4 outlines the PCI DSS responsibilities for the customer.

Table 4. Payment Card Industry Data Security Standards Responsibilities

Control Objective	PCI Requirements	Reference
Build and maintain a secure network.	1. Install and maintain a firewall configuration to protect cardholder data.	Network
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.	Access and Authorization
Protect cardholder data.	3. Protect stored cardholder data.	Access and Authorization
	4. Encrypt transmission of cardholder data across open, public networks.	Data Encryption and Key Management
Maintain a vulnerability management program.	5. Use and regularly update antivirus software on all systems commonly affected by malware.	Change Management
Implement strong access control measures.	6. Develop and maintain secure systems and applications.	Configuration Management
	7. Restrict access to cardholder data by business need to know.	Access and Authorization
	8. Assign a unique ID to each person with computer access.	Access and Authorization
Regularly monitor and test networks.	9. Restrict physical access to cardholder data.	Physical Access
	10. Track and monitor all access to network resources and cardholder data.	Monitoring and Logging
Maintain an information security policy.	11. Regularly test security systems and processes.	Business-Continuity Management
	12. Maintain a policy that addresses information security.	Change Management

Table 5 outlines the ISO 27001 responsibilities for the customer.

Table 5. International Organization for Standardization 27001 Responsibilities

Domain	ISO 27001 Requirements	Reference
Context of the organization	4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the information security management system 4.4 Information security management system	Business-Continuity Management
Leadership	5.1 Leadership and commitment 5.2 Policy 5.3 Organizational roles, responsibilities, and authorities	Business-Continuity Management
Planning	6.1 Actions to address risks and opportunities 6.2 Information security objectives and planning to achieve them	Business-Continuity Management
Support	7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Communication	Incident Response

Domain	ISO 27001 Requirements	Reference
	7.5 Documented information	
Operation	8.1 Operational planning and control 8.2 Information security risk assessment 8.3 Information security risk treatment	Physical Access
Performance evaluation	9.1 Monitoring, measurement, analysis, and evaluation 9.2 Internal audit 9.3 Management review	Monitoring and Logging
Improvement	10.1 Nonconformity and corrective action 10.2 Continual improvement	Business-Continuity Management
Annex A controls	Controls that should be considered by the organization	Access and Authorization

Table 6 outlines the SOC 2 responsibilities for the customer.

Table 6. Service Organization Controls 2 Responsibilities

SOC 2 Common Criteria	Security	Availability	Reference
CC1.2 Organization and Management	Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.	Responsibility and accountability for developing and maintaining the entity's system availability and related security policies, and changes and updates to those policies, are assigned.	Change Management
CC1.3 Organization and Management	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.	Business-Continuity Management
CC1.4 Organization and Management	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting availability and security have the qualifications and resources to fulfill their responsibilities.	Business-Continuity Management
CC2.1 Communications	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	The entity has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	Business-Continuity Management
CC2.2 Communications	The security obligations of users and the entity's security commitments to users are communicated to authorized users.	The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	Business-Continuity Management
CC2.3 Communications	The security obligations of users and the entity's security commitments to users are communicated to authorized users.	The availability and related security obligations of users and the entity's availability and related security commitments to users are communicated to authorized users.	Access and Authorization
	Responsibility and accountability for the entity's system security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Responsibility and accountability for the entity's system availability and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Business-Continuity Management
CC2.5 Communications	The process for informing the entity about breaches of the system security and for submitting complaints is communicated to authorized users.	The process for informing the entity about system availability issues and breaches of system security and for submitting complaints is communicated to authorized users.	Incident Response
CC2.6 Communications	Changes that may affect system security are communicated to	Changes that may affect system availability and system security are	Change Management

SOC 2 Common Criteria	Security	Availability	Reference
	management and users who will be affected.	communicated to management and users who will be affected.	
CC3.1 Risk Management and Design and Implementation of Controls	Procedures exist to identify potential threats of disruption to systems operation that would impair system security commitments and to assess the risks associated with the identified threats.	Procedures exist to identify potential threats of disruptions to systems operation that would impair system availability commitments and to assess the risks associated with the identified threats.	Incident Response
	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	Data Protection and Privacy
CC3.2 Risk Management and Design and Implementation of Controls	The entity's security policies are established and periodically reviewed and approved by a designated individual or group.	The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.	Access and Authorization
	Responsibility and accountability for the entity's system security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Responsibility and accountability for the entity's system availability and related security policies, and changes and updates to those policies, are communicated to entity personnel responsible for implementing them.	Change Management
CC3.3 Risk Management and Design and Implementation of Controls	Environmental, regulatory, and technological changes are monitored and their effect on system security is assessed on a timely basis, and policies are updated for that assessment.	Environmental, regulatory, and technological changes are monitored, and their effect on system availability and security is assessed on a timely basis; policies are updated for that assessment.	Business-Continuity Management
CC4.1 Monitoring	The entity's system security is periodically reviewed and compared with the defined system security policies.	The entity's system availability and security performance are periodically reviewed and compared with the defined system availability and related security policies.	Configuration Management
	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.	There is a process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system availability and related security policies.	Change Management
CC5.1 Logical and Physical Access	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Logical access security measures to restrict access to information resources not deemed to be public.	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Logical access security measures to restrict access to information resources not deemed to be public.	Access and Authorization
	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	Data Protection and Privacy
	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Distribution of output restricted to authorized users.	e. Restriction of access to offline storage, backup data, systems, and media.	Access and Authorization
	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Restriction of access to offline storage, backup data, systems, and media.	f. Restriction of access to system configurations, superuser functions, master passwords, powerful utilities, and security devices (for example, firewalls).	Access and Authorization
	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Restriction of access to system configurations, superuser functions, master passwords, powerful utilities, and security.	–	Access and Authorization

SOC 2 Common Criteria	Security	Availability	Reference
CC5.2 Logical and Physical Access	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Registration and authorization of new users.	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Registration and authorization of new users.	Access and Authorization
	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: The process to make changes and updates to user profiles.	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: The process to make changes and updates to user profiles.	Access and Authorization
CC5.3 Logical and Physical Access	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Identification and authentication of users.	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Identification and authentication of users.	Access and Authorization
CC5.4 Logical and Physical Access	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Registration and authorization of new users.	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: Registration and authorization of new users.	Access and Authorization
	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: The process to make changes and updates to user profiles.	Procedures exist to restrict logical access to the defined system, including, but not limited to, the following matters: The process to make changes and updates to user profiles.	Access and Authorization
CC5.5 Logical and Physical Access	Procedures exist to restrict physical access to the defined system, including, but not limited to, facilities, backup media, and other system components, such as firewalls, routers, and servers.	Procedures exist to restrict physical access to the defined system, including, but not limited to, facilities, backup media, and other system components, such as firewalls, routers, and servers.	Physical Access
CC5.6 Logical and Physical Access	Procedures exist to protect against unauthorized access to system resources.	Procedures exist to protect against unauthorized access to system resources.	<ul style="list-style-type: none"> • Access and Authorization • Physical Access
CC5.7 Logical and Physical Access	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	<ul style="list-style-type: none"> • Access and Authorization • Physical Access
CC5.8 Logical and Physical Access	Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.	Procedures exist to protect against infection by computer viruses, malicious codes, and unauthorized software.	<ul style="list-style-type: none"> • Access and Authorization • Physical Access
CC6.2 System Operations	Procedures exist to identify, report, and act upon system security breaches and other incidents.	Procedures exist to identify, report, and act upon system availability issues and related security breaches and other incidents.	Incident Response
	Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.	Procedures exist to provide that issues of noncompliance with system availability and related security policies are promptly addressed and that corrective measures are taken on a timely basis.	Configuration Management
CC7.1 Change Management	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system availability and related security policies.	Access and Authorization
CC7.2 Change Management	Procedures exist to maintain system components, including configurations consistent with the defined system security policies.	Procedures exist to maintain system components, including configurations consistent with the defined system availability and related security policies.	Configuration Management

SOC 2 Common Criteria	Security	Availability	Reference
CC7.4 Change Management	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	Change Management
	Procedures exist to provide that emergency changes are documented and authorized timely.	Procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval).	Change Management
A1.1 Additional Criteria for Availability	–	Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	Business-Continuity Management
	–	Measures to prevent or mitigate threats have been implemented consistent with the risk assessment when commercially practicable.	Business-Continuity Management
	–	Procedures exist to provide for backup, offsite storage, restoration, and disaster recovery consistent with the entity's defined system availability and related security policies.	Storage
	–	Procedures exist to provide for the integrity of backup data and systems maintained to support the entity's defined system availability and related security policies.	Storage

Appendix: Frequently Asked Questions

Q: Can Cisco provide access to bastion host logs in real time? Can a client see who is actively logged into their environment? Can Cisco send bastion logs on a regular basis?

A: No.

Q: What is the security mechanism to protect our internal environment – PCs, and such?

A: Cisco workstations are centrally managed via Cisco's IT tools and policies. This includes the things you would expect (forced workstation locking, antivirus, disk encryption), and is probably detailed in some Cisco IT policy document.

Q: Where are the people specifically who are monitoring, have access to, or will be doing any work on our cloud, located? Where may they be located in the future?

A: Our operations engineers are globally distributed.

Q: Can we host our MCP server in their DMZ?

A: The internal orchestration backbone does need to be a shared layer-2 and layer-3 segment between all systems, both controllers and hypervisors. It would require some nontrivial re-architecture to enable an additional hop between controllers and hypervisors.

Additionally, it's worth noting that this would not be a productive place for a layer of security segmentation. The controllers, by definition, require access to all cloud components in order to manage the environment. So it would not be possible to place the hypervisors behind an additional segmentation layer that added any meaningful limitation without disabling the environment.

Q: Where does Cisco store the various logs? (Are OpenStack logs local to controller nodes on-premises)?

A: OpenStack logs are both stored locally within the AZ, and are streamed to our central log aggregation and analysis systems. This facilitates our diagnostics, capacity planning, and operational services.

The OpenStack logs do not contain what is generally considered sensitive information:

- Projects and instances are referred to by their UUIDs rather than by their human-readable names.
- IP addresses of instances may appear in logs, but these are generally internal-only addresses.
- Credentials are never logged.
- Images are never copied offsite.
- The memory contents, root disks, and volumes of instances are never copied offsite.

Q: How does Cisco block staff from uploading any malicious code, or bad images?

A: All code deployed to customer environments must first go through our testing and validations processes, including approval by multiple engineers. OSSEC is used to detect any changes to production systems being made outside these channels.

Q: Is it possible to remove permissions for Cisco staff to upload any images over SSH, and have a TDA employee do it?

A: We don't generally upload images to Glance. We usually offer a small catalog of sample images to get people started immediately, but we would be happy to forgo that if desired.

We do offer a stream of OpenStack logging to the customer's syslog server. I believe that this should include any Glance uploads, so if a Cisco engineer were to ever upload an image that would be visible to the customer.

Q: Regarding OSsec, can a customer provide some specific config elements to meet their internal policies?

We would be happy to look at their suggestions, but we could not commit to including their config, or to incorporating any future changes they propose.

Q: Can Cisco share its OSsec logs?

A: No.

Q: Can a customer monitor the OSsec in real time?

A: No.

Q: Can we escrow SSH keys?

A: No.

Q: How does Cisco prevent staff from logging in when there is no specific event requiring it?

A: We do not. OSSEC is used to detect any unauthorized changes made, but we do not preemptively restrict the ability of our engineers to access production environments.




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)