



Cisco ServiceGrid

Architecture and Security V1.6



This document is intended to provide clients with an overview of the application architecture, technical infrastructure, security, availability, and continuity measures of Cisco® ServiceGrid™.

ServiceGrid™ is a registered Trademark. The ServiceGrid Core is covered by the US Patent 8,468,233 B1, issued: 06/18/2013.



Contents

| | | |
|-----------|---|-----------|
| 1. | Application Architecture | 5 |
| 1.1 | Layers and Service Processes | 5 |
| 1.2 | Processes, Data, and Control Flow | 6 |
| 1.2.1 | B2B Connections and Online Access | 6 |
| 1.2.2 | Basic Procedure: Double Translation | 6 |
| 1.2.3 | Process and Data Flow Map | 7 |
| 1.3 | Software Components Used | 9 |
| 1.3.1 | Software Architecture | 9 |
| 1.3.2 | Code Layers | 9 |
| 1.3.3 | ServiceGrid Code Modular Structure | 10 |
| 1.3.4 | ServiceGrid Application Security Perimeters | 11 |
| 1.3.5 | ServiceGrid Components | 12 |
| 1.3.6 | Code Structure and Volume | 13 |
| 1.3.7 | Middleware Components | 13 |
| 1.3.8 | Libraries Used | 14 |
| 1.4 | Data Base and Data Objects | 15 |
| 1.4.1 | Data Base Structure | 15 |
| 1.4.2 | Common, Shared and Private Data | 16 |
| 1.4.3 | Data Objects | 17 |
| 1.4.4 | Data Object and Content | 18 |
| 1.4.5 | Common Characteristics of Data Objects | 19 |
| 2 | Technical Infrastructure | 20 |
| 2.1 | Platform | 20 |
| 2.2 | Test and Production Environments | 20 |
| 2.3 | Test and Production Options for Clients | 20 |
| 2.3.1 | Public Cloud (Standard) | 21 |
| 2.3.2 | Private Cloud Solution | 21 |
| 2.4 | Data Centers | 22 |
| 2.4.1 | Locations of Public Data Centers | 22 |
| 2.4.2 | Data Center Environment in Vienna | 22 |
| 2.4.3 | Data Center Environment San Jose | 23 |
| 2.5 | Platform Architecture | 25 |
| 2.5.1 | Zones and Servers | 25 |
| 2.5.2 | Application Processes and Zones | 25 |
| 2.5.3 | Operating System and Utilities Used | 26 |



| | | |
|----------|--|-----------|
| 2.5.4 | Certificates Used | 26 |
| 2.6 | Network | 27 |
| 2.6.1 | Internal Network Layout | 27 |
| 2.6.2 | External Addresses | 27 |
| 2.7 | Load Balancing and Clustering | 28 |
| 2.8 | Scalability of Infrastructure | 29 |
| 2.8.1 | Essential System Parameters | 29 |
| 2.8.2 | Essential System Components and Sizing Options | 30 |
| 2.8.3 | Monitored Values and Reference Profiles | 30 |
| 3 | Technical Operation | 31 |
| 3.1 | Tools and Methods Used | 31 |
| 3.2 | Cloud Control Center (CCC) | 31 |
| 3.2.1 | Technology Used | 31 |
| 3.3 | Monitoring and Alerting | 32 |
| 3.3.1 | Objectives | 32 |
| 3.3.2 | Technology Used | 32 |
| 3.3.3 | Infrastructure Monitoring | 32 |
| 3.3.4 | Application and Process Monitoring | 32 |
| 3.3.5 | Alerting | 33 |
| 3.3.6 | Tactical Monitoring and Strategic Monitoring | 33 |
| 3.3.7 | Tactical Monitoring | 33 |
| 3.3.8 | Strategic Monitoring / Reporting | 34 |
| 3.4 | Availability Reporting | 34 |
| 3.4.1 | Technology Used | 34 |
| 3.5 | Capacity, Availability, Continuity | 35 |
| 3.5.1 | Possible Outage Scenarios | 35 |
| 3.5.2 | Redundant Infrastructure | 35 |
| 3.5.3 | Data Backup | 36 |
| 3.5.4 | Recovery | 37 |
| 4 | Security | 38 |
| 4.1 | ServiceGrid Platform | 38 |
| 4.1.1 | Defense | 38 |
| 4.1.2 | Database Access | 40 |
| 4.2 | Connectivity | 40 |
| 4.2.1 | Transaction Based B2B Data Exchange | 41 |
| 4.2.2 | Online Access | 41 |
| 4.2.3 | Encryption Using HTTPS (SSL) | 44 |



| | | |
|----------|--|-----------|
| 4.2.4 | Tunneling via IPSec | 44 |
| 4.3 | Environment, Data Centers..... | 44 |
| 4.3.1 | Scope | 44 |
| 4.3.2 | Defense | 44 |
| 4.4 | Environment, Office..... | 45 |
| 4.4.1 | Scope | 45 |
| 4.4.2 | Defense | 45 |
| 5 | Data Privacy | 46 |
| 5.1 | ServiceGrid Application..... | 46 |
| 5.1.1 | Data Managed and Stored within the ServiceGrid Application | 46 |
| 5.1.2 | Location of Platforms and Data..... | 46 |
| 5.1.3 | Secure Transport of Data..... | 47 |
| 5.1.4 | Secure Access to Data and Functions..... | 47 |
| 5.1.5 | Secure Storage of Data..... | 47 |
| 5.1.6 | Access and Usage of Data..... | 47 |
| 5.1.7 | Update of Change of Customer Data..... | 48 |
| 5.1.8 | Deletion or Anonymizing of Data..... | 48 |
| 6 | Internal Control System..... | 49 |
| 6.1 | Environment | 49 |
| 6.2 | External Assumptions at Client Side..... | 49 |
| 6.3 | Monitoring..... | 50 |
| 6.4 | Structure and Framework..... | 50 |
| 7 | Appendix | 52 |
| 7.1 | URLs and Services | 52 |
| 7.2 | Private Platform Configuration | 53 |



1. Application Architecture

1.1 Layers and Service Processes

The architecture of the Cisco ServiceGrid platform is based on six layers.

1. The top layer is where customers can access the ServiceGrid application for data management and customization.
2. The second layer implements the ServiceGrid application itself and consists of all ServiceGrid software components.
3. The Middleware Layer contains all system components necessary to run the ServiceGrid programs.
4. The Operating System (OS) Layer implements the OS platform and low level utilities.
5. The Hardware and Network Layer provides the server and network infrastructure.
6. The Data Center Layer provides the location to operate the infrastructure in a safe environment.

For each layer, service processes are in place. The top layer (usage, data management, and customization of the application) is used by the Cisco ServiceGrid customers and supported by Cisco ServiceGrid support and services.

All other layers are operated and supported by Cisco. (See Figure 1)

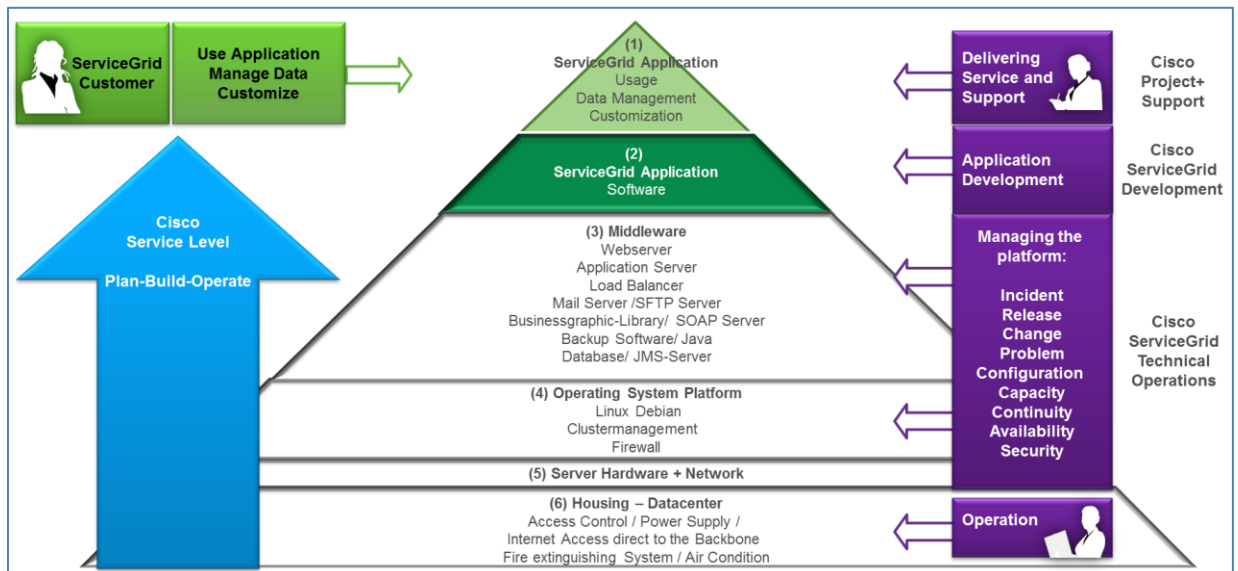


Figure 1. Platform Layers and Service Processes



1.2 Processes, Data, and Control Flow

1.2.1 B2B Connections and Online Access

The Cisco ServiceGrid application provides modules and functions for web based service management together with various B2B connection methods for the integration of service partners.

Basic data as well as service call data is stored and managed in a central database. This enables a combined usage of transactions based B2B connections and web based ticket handling. (See Figure 2)

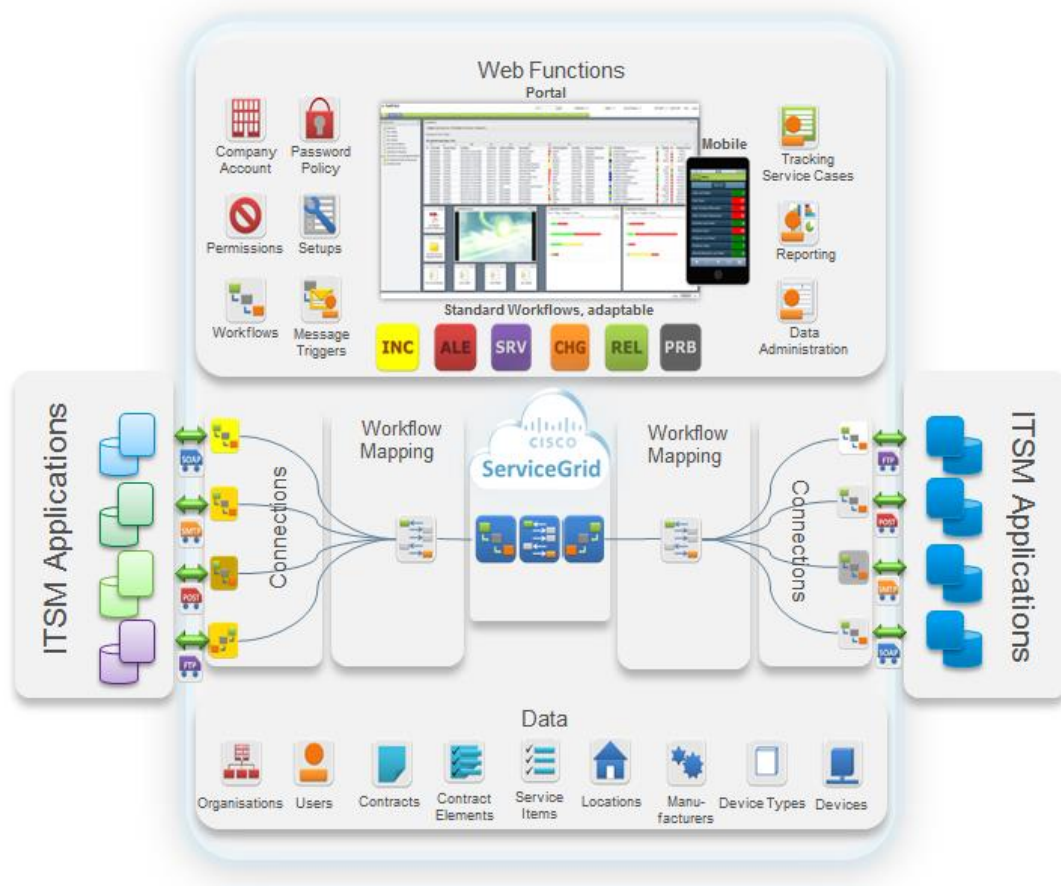


Figure 2. Web based online modules for service management and B2B connectors to integrate service partners

1.2.2 Basic Procedure: Double Translation

In order to connect Ecosystem Trading Partners' processes and workflows, Cisco ServiceGrid uses the principle of double translation. Incoming data is mapped from the customer specific format to the normalized format and then to the receiver specific format. This is how ServiceGrid provides one-to-many and many-to-many connections to create an ecosystem.

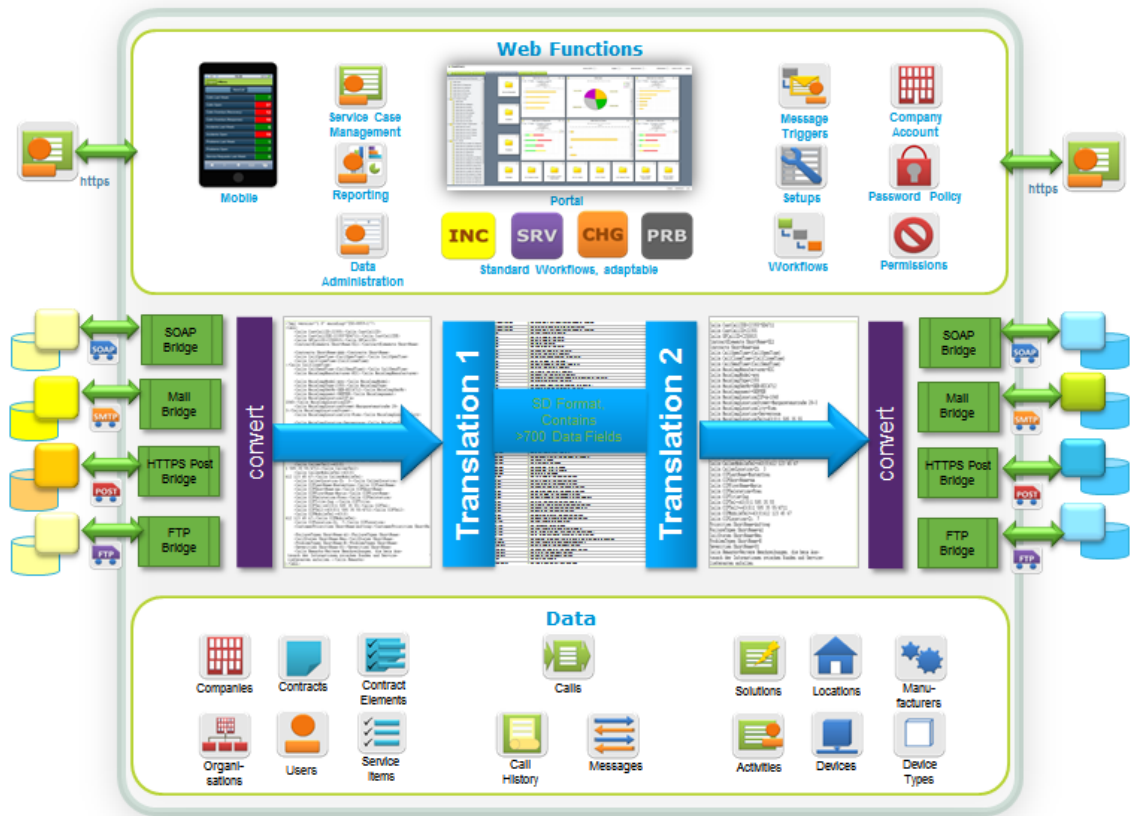


Figure 3. ServiceGrid: Principle of Double Translation

Workflow mappings between Ecosystem Trading Partners are defined in the workflow settings in the data base objects. Those settings (Status Codes, Transaction Types and Field Mappings) are customized for the Ecosystem Trading Partner connections and are used to translate and store inbound transactions into the ServiceGrid Call Data Object and to generate the required outbound transaction from the ServiceGrid Call Data Object.

Service requests created in the ServiceGrid online web interface are also processed into the same Call Data Object. This allows a combined usage of web based service management and B2B connections between Ecosystem Trading Partners. (See Figure 3)

1.2.3 Process and Data Flow Map

Cisco ServiceGrid consists of a set of processes communicating via a set of dedicated message queues. The web based online functions access the data via the ServiceGrid Data Base Framework. All ServiceGrid software components are implemented in Java. (See Figure 4)

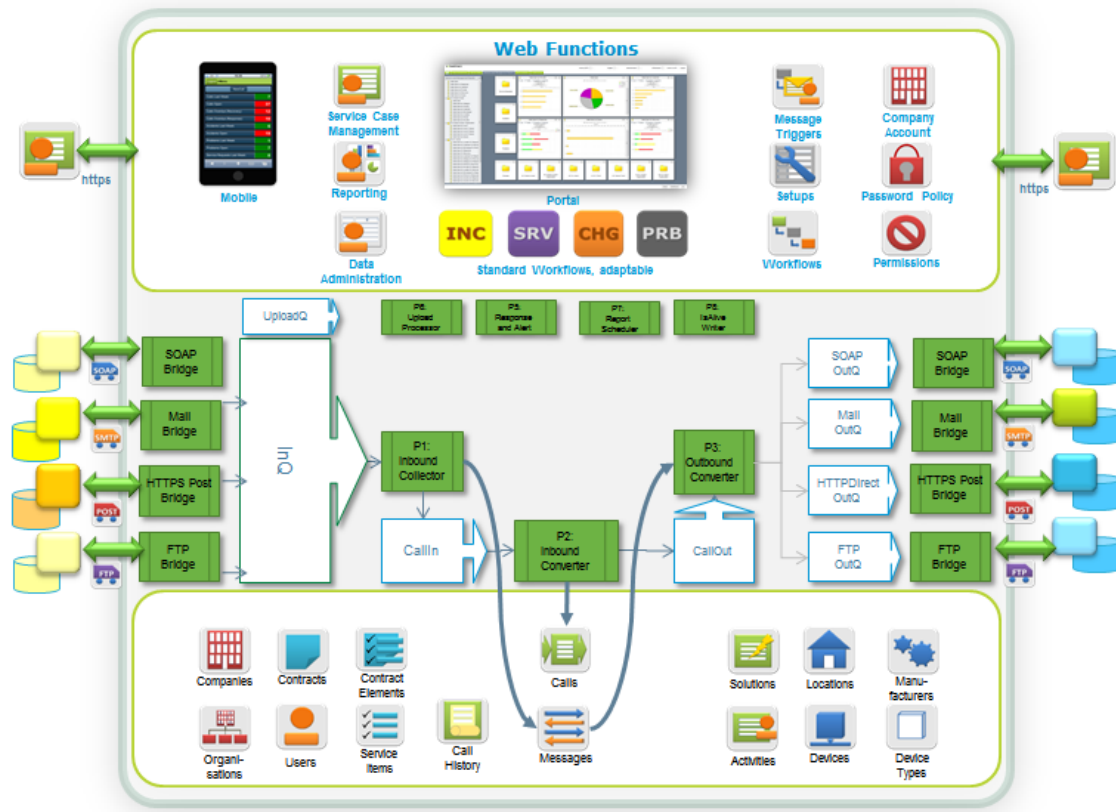


Figure 4. Processes, Message Queues and Data Base

ServiceGrid Web Interface

The web based online functions are organized as a set of modules and are executed in a run time environment provided by Apache Web Server and Tomcat application server.

ServiceGrid B2B Connections

The ServiceGrid B2B functions consist of dedicated B2B connections for the various communication methods. Inbound messages addressed to the specific service are processed via the InQueue to the Inbound Collector. The Inbound Collector runs the authentication procedure and – if successful - stores the message in the data base and passes the data via the CallIn Queue to the Inbound Converter.

The Inbound Converter maps the content into the ServiceGrid Call Data Object (Translation 1). In case an outbound transaction has to be triggered, the Call Data is pushed to the CallOutQueue. The Outbound Converter generates the outbound message in the defined format (Translation 2), stores the message in the data base and pushes the message to the dedicated outbound queue.



1.3 Software Components Used

1.3.1 Software Architecture

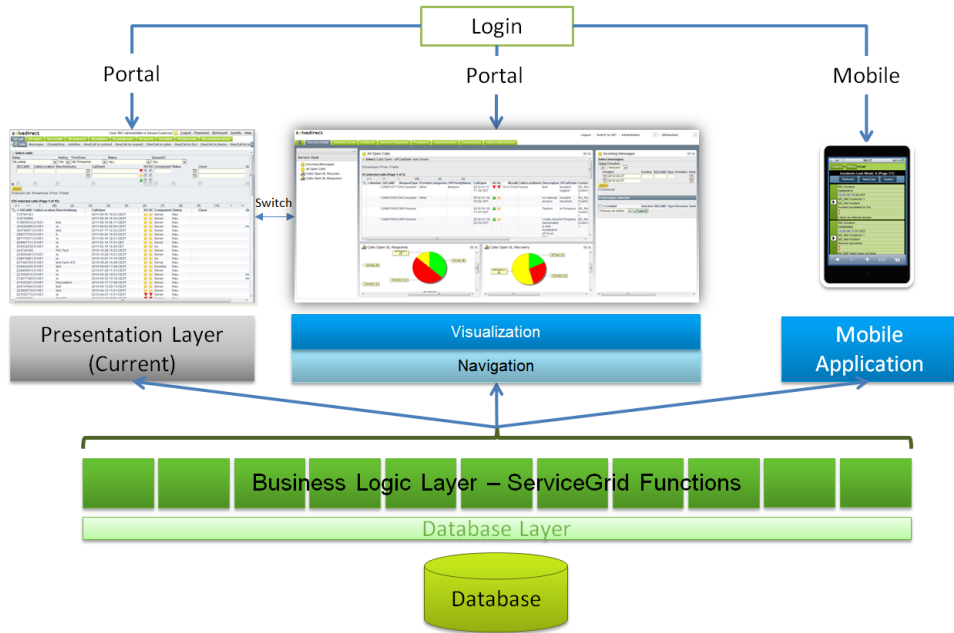


Figure 5. Software Architecture

1.3.2 Code Layers

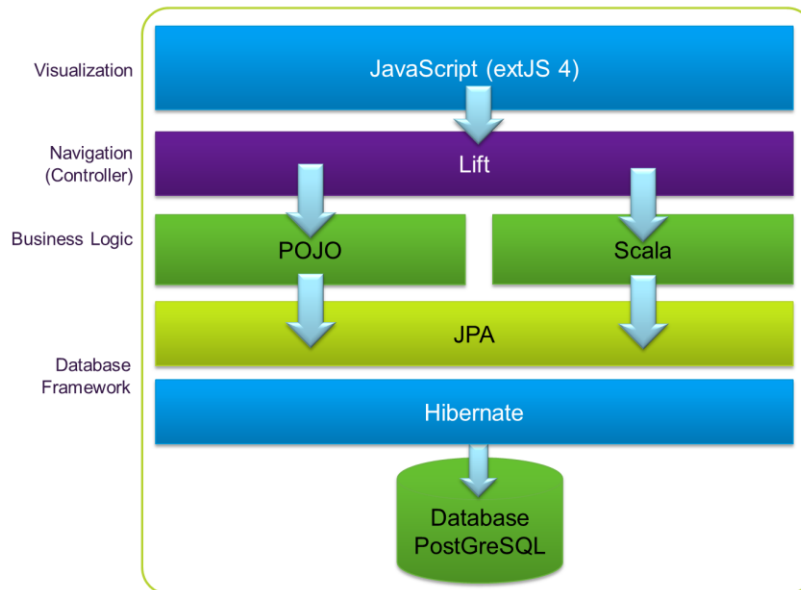


Figure 6. Code Layers



1.3.3 ServiceGrid Code Modular Structure

Static Content is everything delivered to the client without server side processing. It contains the underlying JavaScript Framework (ExtJS), extensions to it, as well as web resources such as images or style sheets. It also contains initialization routines for starting up the web application such as the deployment descriptor and bootstrap filters. (See Figure 7)

User Interface Service Endpoints contain the services that can be called by the client. These are differentiated into two types: synchronous services, providing complete HTML pages in form of Lift Snippets and asynchronous services in the form of restful web services using Lift internal stateful dispatch functions. This module has access to the web request and prepares data for further usage. (See Figure 7)

Transformation Modules transform data received from the client into abstract entity instances and vice versa. This transformation is necessary to represent ServiceGrids' setup able fields. These abstract entity instances can be enriched with additional metadata such as constraints. (See Figure 7)

Business Logic Modules execute business operations. They are responsible for doing complex calculations such as checking interdependencies between certain fields, SLA calculation, or computation of business critical timestamps. Another task of these modules is the creation of dynamic views out the default views and setup definitions. (See Figure 7)

Metadata is the fundamental framework that creates views on entities with additional features that cannot easily be represented directly in the entity itself. It contains the logic for creating, writing, and reading entities in an independent way of the underlying OR-Mapper. (See Figure 7)

At the bottom of this diagram one can find the entities which represent type and relations of data stored in the database. This module also contains default views over entities.

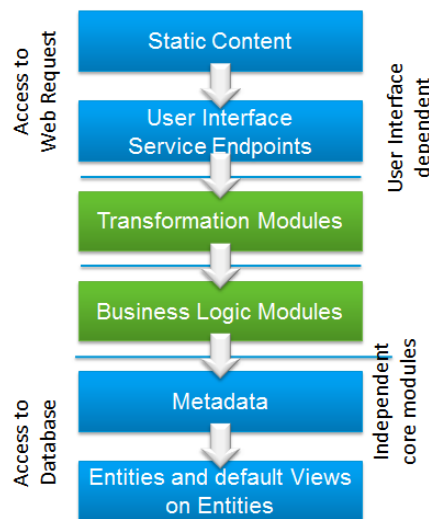


Figure 7. Code Modular Structure



1.3.4 ServiceGrid Application Security Perimeters

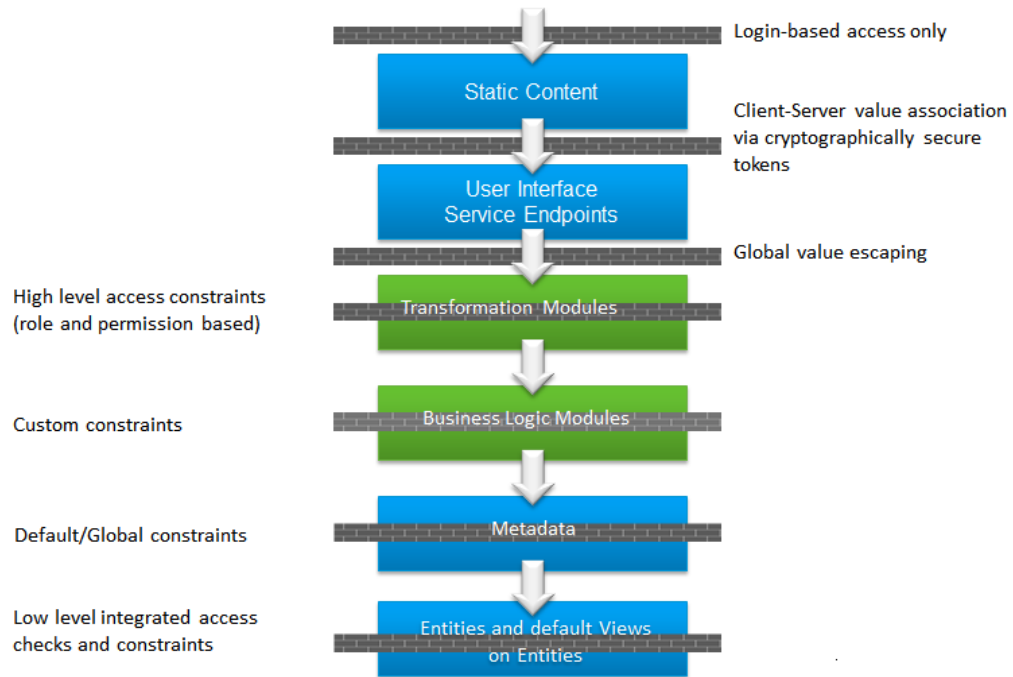


Figure 8. ServiceGrid Application Security Perimeters

Table 1: Security Perimeters

| Parameters | Description |
|--|---|
| Login based access only | The ServiceGrid application is available to authenticated users only. |
| Client-Server value association via cryptographically secure tokens | All values which have representations on both the client and the server are associated via cryptographically secure tokens, such as IDs, form fields, buttons, windows or anything else. Not only does this prevent iterating through IDs but makes any form of session replay impossible, even if data were accessed via an SSL MITM attack. |
| Global value escaping | The framework ensures that only valid values may pass between client and server. Any value is „deeply validated“, including XML and JSON. This ensures a “global whitelist“, making XSS ² and CSRF ³ impossible by design. |
| High level access constraints | A complex role- and group-based permission scheme where access levels may be inherited through hierarchies of folders allows meeting highest user demands while still being confined by lower level checks, should something be missed. |
| Custom constraints | Custom constraints allow restricting possible values specific to this view. This enables maximum flexibility for the user and the tightest constraints possible (e.g. “in this view, only allow devices which have a specific DeviceType” or “this phone number must have the format X”). |
| Default/Global constraints | Default/Global constraints specify globally valid constraints on single fields as well as complete views, from “only allow to reference devices of my company” via “only call states of the current call system” to “serial number may only contain letters and numbers”. These are implemented once and checked on every access, so cannot be circumvented by individual code. |
| Low level integrated access checks | Low level integrated access checks restrict the access of the code to a basic set of data via automatic low level mechanisms. No individual implementation necessary, so no errors to be introduced. |

MITM Man in the Middle ² XSS Cross Site Scripting ³ CSRF Cross Site Request Forgery



1.3.5 ServiceGrid Components

The various ServiceGrid application processes implement the functions shown in Table 2.

Table 2: Service Components

| Application Process | Function |
|---------------------------|---|
| ServiceGrid online | ServiceGrid online modules: <ul style="list-style-type: none"> • SG.call • SG.mobile • SG.calendar • SG.solutions • SG.basicdata • SG.commoncontent • SG.inventory • SG.databroker • SG.cockpit |
| P1 | Inbound collector: <ul style="list-style-type: none"> • reads incoming messages from the InQ • checks the proper authentication • stores the message in the data base • push the message into the CallIn queue |
| P2 | Inbound converter <ul style="list-style-type: none"> • reads messages from the CallIn queue • processes the message: <ul style="list-style-type: none"> ○ converts the message into the ServiceGrid Call format ○ stores the call in the data base ○ into the CallOut queue • or (if the message cannot be converted) <ul style="list-style-type: none"> ○ creates an error message ○ and push the error message into the CallOut queue |
| P3 | Outbound message converter <ul style="list-style-type: none"> • reads the Call or the error message from the CallOut queue • converts the Call or error message from the ServiceGrid format into the receiver format • stores the translated Call or error message as message in the data base • stores alert timestamps in the data base • push the translated Call or error message as message into the assigned OutQ |
| P5 | Response and alert processor <ul style="list-style-type: none"> • reads the list of scheduled alerts from the data base • checks which alerts are still valid • fires the alert • push the Call data into the CallOut queue |
| P6 | Upload processor <ul style="list-style-type: none"> • reads the uploaded data objects • checks the authentication • processes the upload |



| | |
|-----------|--|
| P7 | Report scheduler updater <ul style="list-style-type: none"> updates the schedule execution information in the data base |
| P8 | IsAlive writer <ul style="list-style-type: none"> send control topic (ping) to all other processes touches IsAlive file for all valid response used for monitoring purposes |

1.3.6 Code Structure and Volume

Table 3 shows detailed information about the code structure and volume.

Table 3: Code Structure and Volume

| | |
|---------------------------------------|--|
| Programming languages employed | Java, Scala, SQL, XSLT, JavaScript |
| History and Evolution of Code | <ul style="list-style-type: none"> DB-Framework created 2001 Converter code implemented 2001, re-implemented 2004 Bridge code implemented 2001, re-implemented 2008 GUI code created 2001, re-implemented 2004, extended 2007, 2009 (more JavaScript) Complete reimplementation of the technology stack started in 2012 <ul style="list-style-type: none"> Programming language: Scala DB Framework: JPA/Eclipse Link Web Framework: Lift GUI Framework: ExtJS |
| Source Code Quality | A set of coding standards is defined and used by the development team: <ul style="list-style-type: none"> How_to_develop_SG Java_Scala_Coding_Style Scala_Coding_Style JavaScript_Coding_Style |
| IP Ownership | The ownership of intellectual property is with Cisco. |

1.3.7 Middleware Components

The ServiceGrid application is runs in the software environment shown in Table 4.

Table 4: Software Environment

| Function | Software | Link |
|---------------------------|-------------------------|--|
| Webserver | Nginx | http://www.nginx.net/ |
| Application Server | Tomcat | http://tomcat.apache.org |
| Mail Server | Postfix | http://www.postfix.org |
| FTP Server | ProFTPD | http://www.proftpd.org |
| SOAP Server | Axis Glassfish Metro | http://ws.apache.org/axis https://metro.dev.java.net/ |



| | | |
|-------------------|------------|---|
| Database | PostgreSQL | http://www.postgresql.org |
| JMS-Server | OpenMQ | https://mq.dev.java.net/ |
| Java | Oracle JDK | http://java.sun.com |

1.3.8 Libraries Used

Table 5 shows the libraries used. None of these libraries are under GPL or AGPL license agreements.

Table 5: Libraries used

| Party | Library | Party | Library |
|----------------|------------------------|-------------|-----------------------|
| Oracle | activation | JBoss | javassist |
| Jetbrains | annotations | Oracle | javax.annotation |
| OWASP | antisamy | atinject | javax.inject |
| AntLR | antlr | Oracle | jaxb-api |
| Sourceforge | aopalliance | Oracle | jaxb-impl |
| OW2 Consortium | asm | Codehaus | jaxen |
| Apache | avalon-framework | JBoss | jboss-logging |
| Apache | axis | JBoss | jboss-transaction-api |
| Apache | axis-jaxrpc | JFreeChart | jcommon |
| Apache | axis-saaj | jdom.org | jdom |
| Apache | axis-sd | Oracle | jersey-core |
| Apache | axis-wsdl4j | Oracle | jersey-json |
| Apache | batik | Oracle | jersey-server |
| Apache | batik-css | Oracle | jersey-servlet |
| Apache | batik-ext | Codehaus | jettison |
| Apache | batik-util | JFreeChart | jfreechart |
| Bouncy Castle | bcmail-jdk14 | Oracle | jms-api |
| Bouncy Castle | bcprov-jdk14 | Sourceforge | joda-time |
| Bouncy Castle | bctsp-jdk14 | Sourceforge | jsch |
| Beanshell | bsh-core | Oracle | jsr-310-ri |
| Sourceforge | cglib | Oracle | jsr-310-TZDB |
| Apache | commons-beanutils | Liftweb | lift-actor |
| Apache | commons-beanutils-core | Liftweb | lift-common |
| Apache | commons-codec | Liftweb | lift-db |
| Apache | commons-collections | Liftweb | lift-json |
| Apache | commons-configuration | Liftweb | lift-mapper |
| Apache | commons-digester | Liftweb | lift-proto |
| Apache | commons-discovery | Liftweb | lift-util |
| Apache | commons-fileupload | Liftweb | lift-webkit |
| Apache | commons-httpclient | Apache | log4j |
| Apache | commons-io | Oracle | mail |



| | | | |
|---------------------|-------------------------------|----------------|-------------------|
| Apache | commons-lang | Sourceforge | mime-util |
| Apache | commons-logging | Sourceforge | nekohtml |
| Apache | commons-net | Ping Identity | opentoken-adapter |
| Apache | commons-validator | Apache | oro |
| Oracle | dbbridge-ojdbc | Codehaus | paranamer |
| Apache | derby | postgresql.org | postgresql |
| Sourceforge | dom4j | Apache | poi-3.8 |
| Davisor | davisorchart | Oracle | rome |
| Terracotta | ehcache | Scala-lang.org | scala-compiler |
| Terracotta | ehcache-jmsreplication | Scala-lang.org | scala-library |
| OWASP | esapi | Scala-lang.org | scalap |
| Sourceforge | flexjson | Scala-lang.org | scala-reflect-sd |
| Apache | fop | Apache | serializer |
| Google | guice | slf4j.org | slf4j-api |
| Google | guice-servlet | slf4j.org | slf4j-log4j |
| H2 | h2 | Codehaus | stax-api |
| JBoss | hibernate-commons-annotations | Oracle | transaction-api |
| JBoss | hibernate-core | Sourceforge | usertype.extended |
| JBoss | hibernate-entitymanager | Sourceforge | usertype.spi |
| JBoss | hibernate-jpa | Oracle | webservices-api |
| Sourceforge | htmlparser | Oracle | webservices-rt |
| Oracle | imq | Cisco | wikiSD |
| Oracle | imqjmx | Apache | xalan |
| iText Software Corp | itext | Apache | xercesImpl |
| Codehaus | jackson-core-asl | Apache | xml-apis |
| Codehaus | jackson-jaxrs | Apache | xml-apis-ext |
| Codehaus | jackson-mapper-asl | Apache | xmlParserAPIs |
| Codehaus | jackson-xc | Oracle | xom |
| Sourceforge | jasperreports | | |
| JBoss | javassist | | |

1.4 Data Base and Data Objects

1.4.1 Data Base Structure

Logical data structure

All data is organized in a relational data base. The logical design of the data follows the requirements of service management data and implements the organizational structure of the Ecosystem Trading Partner, the inventory data, the service catalog data and the service cases as calls (for example incidents, problems, changes).



Physical data structure

The physical data structure consists of more than 300 entities and relations. Access from the programs to the physical data structure is implemented via JPA/Hibernate for the ServiceGrid data base framework. The framework implements the relation between logical and physical data structures and the access rights to private, shared, and common data. (See Figure 9)

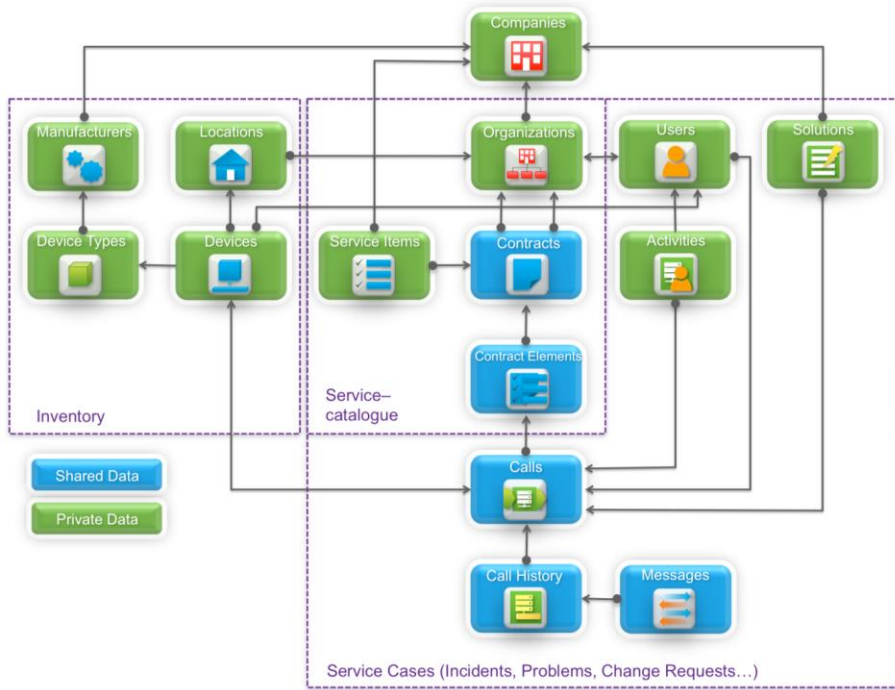


Figure 9. Logical Data Design (Simplified E-R Diagramm)

1.4.2 Common, Shared and Private Data

Data is divided in private data, shared data and common data. Each company on the ServiceGrid platform has a company record describing the company account. The data in the database is organized by company accounts, meaning each record in a table containing company-specific private data:

- is referenced to the company (account)
- can only be viewed by an authorized user who is a member of the company account.

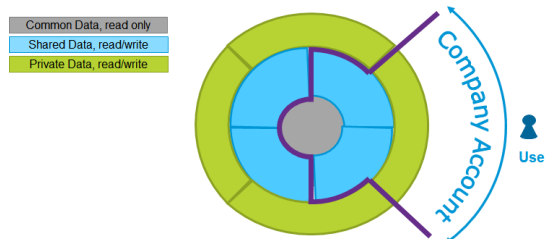


Figure 10. Company Account and Private, Shared and Common Data



1.4.3 Data Objects

The company record has a unique ID. Private data records are referenced to the unique company record. Shared data records are referenced to exactly two company accounts as Service Provider and Service Customer.

The ServiceGrid Data Base Framework assures that access to private data records is only granted to users being member of the company and access to shared data records is only granted to users being member of the Service Provider or the Service Customer Company. (See Table 6)

Table 6: Data Objects

| Data Object | |
|--------------------------|--|
| Companies | Private |
| Organizations | Private; can be shared with connected partners |
| Queues | Private |
| Users | Private; can be shared with connected partners |
| Locations | Private; can be shared with connected partners |
| Service Items | Private |
| Devices | Private; can be shared with connected partners |
| Activities | Private |
| Messages | Private |
| Solutions | Private; can be shared with connected partners |
| Surveys | Private |
| Contracts | Shared |
| Contract Elements | Shared |
| Calls | Shared |
| Countries | Common |
| Time Zones | Common |
| Languages | Common |



1.4.4 Data Object and Content

Table 7: Data object descriptions

| Data Object | Description |
|--------------------------|---|
| Companies | Each company on the ServiceGrid platform has a company record. The company may have one or more organizations. Within an organization there may be a number of locations. A company always belongs to one country and one time zone. Each company has one user as contact person. Solutions, Queues and call systems belong to the company. The company is the root record for ServiceGrid customers (the account). All information about the structure of a company including organizations, users, and workflows are referenced to the company record. |
| Organizations | Each company consists of one or more organizations. Service contracts are always concluded between organizations. Depending on the contracts, organizations act as service provider organization (e.g. incident management, problem management) or as service customer organization (e.g. certain departments, regions or external companies having service contracts with the different service organizations). |
| Queues | The function of a queue is to route calls to certain skills. Queues apply directly to companies and can hold an unlimited number of technicians. Queues can be structured into three levels (Level 1/2/3) and can be assigned to specific workflows. The queue selection can be pre-set in the Contract Elements and appears (by default) when opening a new call. |
| Users | Users are all persons participating in the service process as administrators of the ServiceGrid platform, as part of the service desk, support, technicians or end-users. A user is member of one or many organizations. A user may have a login/password to the ServiceGrid platform or is only referenced as end user or contact person and has no personal login. Each user has access only to data of his organization and only permissions according to his permission group. Service desk and service support users are all persons who are active participants in the service process as service desk, helpdesk or 2nd-Level persons. Service desk and service support users have usually login/password. End users are users which may be referenced to a call as a caller or contact person. End users may have a login/password and are only enabled to view their own calls. |
| Locations | Locations are addresses of places where services have to be delivered or devices are installed. Locations belong to exactly one (in most cases customer) organization. |
| Contracts | A contract describes the relation between service customer and service provider. A contract may or may not include inventory. A contract may contain one or more contract elements. Calls are uniquely related to one specific contract element. |
| Contract Elements | Contract elements are the services provided for a specific customer organization by a specific provider organization. Contract elements are elements of service contracts and may define all attributes of the service agreement. Contract elements hold information about service level agreements, escalation rules, categorization and escalation to queues. |
| Service Items | Service items are the provided services and hold all attributes of a service including service level agreements, escalation rules, categorization and escalation to queues, but have initially no reference to a contract. When a service delivery contract is agreed between customer and provider, the service item is referenced to the contract. |
| Devices | Devices (Hardware, Software, Documents) are referenced to exactly one device type, exactly one organization, and exactly one location. Each device has a referenced service level within a contract. A device may have a user as an owner. |
| Calls | Calls are the main data objects and contain the summary of all service requests in terms of incidents, problems, change requests or plain service requests. Each call is referenced to exactly one service customer organization and one service provider organization using a reference to a contract element within a contract. A call may also be referenced to one or many devices, to persons (caller, helpdesk, contact, technicians) and to locations. |
| Activities | Activities are created by the person working on the call and may contain work time data, travel time data and distance. Activities are used to document the planned and/or fulfilled effort during the work on service requests. |
| Messages | Messages are data records (text, XML, csv) sent (outbound) to external applications or persons or received (inbound) from external applications or persons. Messages are referenced to exactly one Call. |



1.4.5 Common Characteristics of Data Objects

Main data objects

- have a unique ID within the company (e.g. the Location Short Name)
- have a small set of mandatory fields in the standard view
- have an internal structure (relations to tables, location country, location devices)
- have standard fields (e.g. name, address,...)
- have a status (e.g. „planned“, „operation“, „closed“)
- (may have) editor, edit time (responsible for last change of data)
- (may have) hierarchical structure (e.g. location hierarchy)
- (may have) history-log (e.g. location-history)
- (may have) extensions (individual additional fields)

The management and administration of data objects is done by

- Customization for each company (views, field extensions, type-codes, status-codes)
- Standard list and detail views for selection, create and update
- Different individual views, depending on permission of user
- Upload and download of data from or into files



2 Technical Infrastructure

2.1 Platform

ServiceGrid is a hosted software solution. Data and applications are stored centrally in a data center and are accessible by the users via the Internet.

The ServiceGrid Portal can be accessed online from any computer with a modern standard internet browser and internet connection. No software or hardware installation is required.

ServiceGrid Mobile can be accessed only from smart phones using a standard internet browser.

Connecting an existing system to the ServiceGrid platform requires no investment in hardware. Each participant of the ServiceGrid platform chooses their own particular interface options (which can be chosen according to security, performance and system requirements) that allow him to interact with the other partners in the ecosystem via a neutral B2B gateway.

2.2 Test and Production Environments

The ServiceGrid platforms are operated out of data centers. ServiceGrid provides three production platforms as public cloud applications to the ServiceGrid customers. These production platforms are operated out of three different data centers:

- Platform sdcall: Data center located in Vienna
- Platform vie2: Data center located in Vienna
- Platform sjc1: Data center located in San Jose, CA

Test and staging platforms are available:

- Platform staging: Test platform dedicated to customers, running the current release (same as on the production platforms)
- Platform test: Beta test platform running the beta release of the upcoming next release

Customers may run their own ServiceGrid platform within their own premises and data centers operated by Cisco.

2.3 Test and Production Options for Clients

The ServiceGrid customer can select one of three options:

- Using one of the ServiceGrid shared platforms
- Host a ServiceGrid private platform operated by Cisco in the client data center
- Let ServiceGrid host a private platform in one of Cisco data centers.



2.3.1 Public Cloud (Standard)

The customer uses one of the shared ServiceGrid platforms in one of the Cisco data centers which provide optimal performance and high security standards.

2.3.2 Private Cloud Solution

The ServiceGrid solution is sold as a Black Box. The servers and systems remain under the control of Cisco even if they are installed at the customer data center. The customer may optionally provide networking and firewall services and only procure dedicated servers.

ServiceGrid Blackbox – Default Requirements

- Rackspace for 25 rack units in a single rack
- Two different power circuits with 12 A power connections on each circuit
- Direct internet uplink (> 5 mbps) with public IP addresses (4 + one additional per each SSL certificate)
- Two Ethernet internet uplink cables (for redundancy)
- Permanent remote network access for Cisco technicians via IPsec.

Network and firewall provided by customer

- Four VLANs for demilitarized, application, data and management zone
- Three cables per server, using LACP for failover and one to access the management interface
- Three IPsec tunnels for configuration management, monitoring and maintenance
- L3 load balancing

2.3.2.1 Private Cloud Hosted in a Cisco data center

The customer uses a private dedicated environment in one of the Cisco data centers. The private environment is dedicated to the client only, and consists of a ServiceGrid production platform and a ServiceGrid test platform (recommended).

Cisco will provide necessary hardware and host it in the Cisco data center. All maintenance is done by Cisco. Hardware sizing depends on the customer requirements.

2.3.2.2 Private Cloud Hosted at the Customer's Data Center

The customer uses a private dedicated environment in its own data center. The private environment is dedicated to the client only, and consists of a ServiceGrid production platform and a ServiceGrid test platform (recommended).

Cisco will provide a bill of material of necessary hardware and the customer can host it in their data center. All maintenance is done by Cisco. Hardware sizing depends on the customer requirements. Please see chapter 2.3.2 for the Blackbox default requirements.

Showstoppers



- No direct or permanent network access for Cisco
- Customer wants access to the operating system
- Customer wants to operate the ServiceGrid platform themselves
- No wildcard certificates available

2.4 Data Centers

2.4.1 Locations of Public Data Centers

In each of the provided data centers, a ServiceGrid platform is operated by Cisco and provided to the ServiceGrid customers.

Each ServiceGrid customer has one or many company accounts on the ServiceGrid platform. Within a company account the customer may manage its private data (company, organizations, users, devices) and may share data (contracts, calls) with other company accounts.

2.4.2 Data Center Environment in Vienna

The data center is located in Vienna, Austria and operated by upstreamNet Communications GmbH.

- Cisco has a colocation contract with upstreamNet including provision of space and connections to the internet.
- The ServiceGrid platform itself is not operated by upstreamNet but by the ServiceGrid technical operations team.
- The ServiceGrid platforms infrastructure (servers and local network components) is installed in rack mounted server boxes inside the data center.

The following infrastructure and facilities are provided by the data center:

Personal access control

Access to the data center follows a three stage access procedure:

- Access to the building is controlled by the building reception staff.
- Access to the data center within the building is only provided for authorized persons and controlled via access lists.
- Access to the locked inner compartment of the data center is always escorted.

All rooms of the data center are permanently monitored per video and motion detectors. All visits are documented.

Internet connection

The data center is partner of AboveNet and therefore directly connected to the AboveNet Backbone. This Network (AS6461) was designed for high scalability, availability, and performance. The AboveNet Backbone connects



Japan, North America, and Europe and has more than 450 peering agreement contracts worldwide. All backbone components are redundant. The network is operated and monitored via the international AboveNet Network operation center on a 24x7 base. ServiceGrid uses a direct connection to the AboveNet Backbone with a flexible bandwidth agreement.

Power supply

Electric power is supplied via two separated lines from the public power network. An UPS facility guarantees an alternative power supply for 30 minutes. Additionally two diesel engines (1,3 MW) can provide a constant power supply. The diesel engines are constantly held in operating temperature and can take over within 30 seconds. Gasoline for 48 hours operation is constantly on stock.

Air condition

The air condition provides a constant temperature of 22 ° Celsius (71.6 ° Fahrenheit) and air humidity of 40 percent. Two refrigerating machines, buffered by an ice container, supply eight cold chambers in the data center. The so generated cool air is directed under floor to the racks.

Fixed fire extinguishing system

A permanent monitoring of the compartment air allows early detection of smoke and will trigger an early alarm. In this case, the air condition will be switched off to prevent further oxygen supply. The following main alarm will trigger the flood of the compartment with FM002 fire extinguish gas. FM002 is not dangerous for humans and equipment.

2.4.3 Data Center Environment San Jose

The data center is located in San Jose, CA, USA and operated by Datapipe, Inc.

- Cisco has a colocation contract with Datapipe, including the provision of space and connections to the internet.
- The ServiceGrid platform itself is not operated by Datapipe but by the ServiceGrid Technical Operations team.
- The ServiceGrid platforms infrastructure (servers and local network components) are installed in rack mounted server boxes inside the data center.

The following infrastructure and facilities are provided by the data center.

- SAS 70 Type II certified, HIPAA Compliant
- Entire structure meets Bellcore Network Equipment Building Systems Requirements
- Carrier neutral facility fed by multiple Tier 1 providers, via redundant MPOE fiber vaults
- DataPipe network features redundant fiber sources, aggregate switches and core routers

**Security and personal access control**

- 24/7 on-site building and network monitoring
- 24/7 security staff, strictly enforced security procedures
- Colo exterior radius structure meets Level III / explosion resistance security standards
- One of the first facilities to implement true three factor security
- Visitors are escorted by authorized personnel at all times
- 24 hour internal and external video surveillance, 60 day minimum retention policy
- Multiple mantraps with reinforced walls

Internet connection

- 100mbps burstable Internet connect, 10 mbps commitment
- Additional bandwidth contracted
- Included 16 Usable IPs

Power supply

- Facility fed by multiple power grids
- Pre-negotiated 1 hour advanced notice contact for any pending rotating block outages
- 5 HiTec rotary flywheel Uninterruptible power supply (UPS) system N+2 architecture
- 5 HiTec generators rated at 1.8 megawatts each with 20,000 gallons of fuel capacity
- Contracted fuel suppliers on call 24 hours a day, seven days a week
- 75 watts per square foot
- 22 PDUs located throughout the data center rated at 225kva each

Air condition

- HVAC Temperature Controlled Environment
- 367 BTUs of cooling per square foot
- Temperature range of 72 +/- 5 degrees Fahrenheit
- Relative humidity range from 40% – 60% RH
- 71 CRAC units rated at 22 tons of cooling, utilizing DX, R-22 refrigerant
- Raised floor to provide uniform cooling distribution

Fixed fire extinguishing system



- VESDA smoke detection systems, above and below raised floor
- Dual interlock pre-action dry-pipe fire suppression system (two events required to activate)
- California Category Four earthquake compliant

2.5 Platform Architecture

2.5.1 Zones and Servers

The ServiceGrid platform is operated in a segmented environment for security and availability reasons.

Each zone is dedicated to a certain group of services following a security layout consisting of three security perimeters. (See section “Security”)

All components which are important for the availability of the system are redundant. Redundancy is implemented through clusters or a multi-server design (See Section “Availability and Continuity”).

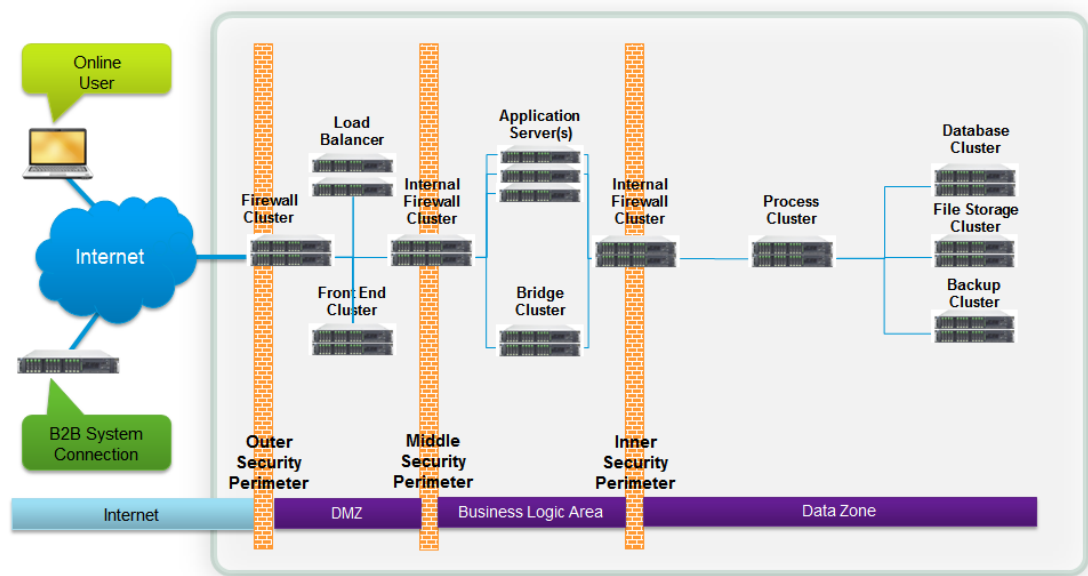


Figure 11. Zones and Servers of the ServiceGrid Platform

2.5.2 Application Processes and Zones

The processes implementing the ServiceGrid application are assigned to dedicated zones. The zones are separated by three security perimeters. Application data is stored in the data zone only.

For details about the perimeters and zones please see Section “Security”.

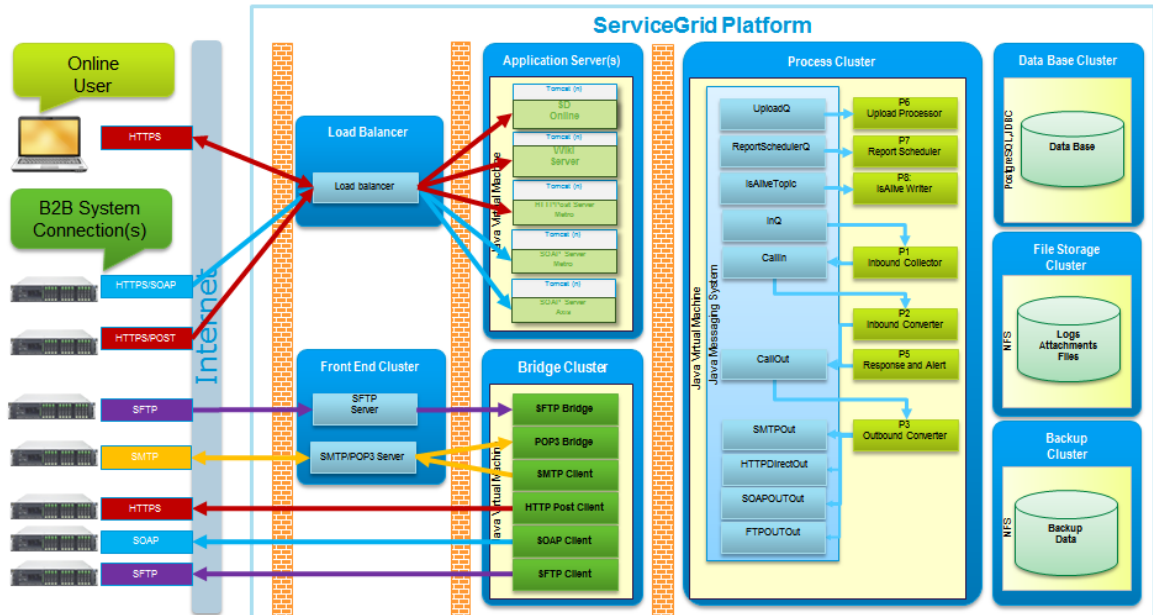


Figure 12. Application Processes and Zones

2.5.3 Operating System and Utilities Used

Table 8: Operating System and Utilities Used

| Function | Software | Link |
|--------------------|------------------------------------|--|
| OS | Debian GNU/Linux | http://www.debian.org |
| Cluster management | Heartbeat | http://www.ha-linux.org |
| Cluster | DRDB | http://www.linbit.com |
| Firewall | Linux iptables | http://www.netfilter.org |
| Load balancer | Linux Virtual Server (LVS) / nginx | http://www.linuxvirtualserver.org http://www.nginx.net/ |

2.5.4 Certificates Used

ServiceGrid uses SSL certificates signed by HydrantID (<https://www.hydrantid.com/>) for its services provided via HTTPS. ServiceGrid can accept any certificate (also self-signed) if it is issued correctly (CN must match, it mustn't be expired, etc.).

ServiceGrid HTTPS B2B connection is able to authenticate itself via a client certificate and our customers may use client certificate to authenticate themselves.



2.6 Network

2.6.1 Internal Network Layout

The network infrastructure is implemented via at least two manageable switches. For security and availability reasons each server is connected via LAN-controller to at least two separate switches.

2.6.2 External Addresses

The ServiceGrid application as a hosted solution is visible from outside (Internet) only via the defined services. All connections to ServiceGrid use encryption by default and need authentication.

Table 9: Encryption

| Access Method | Authentication | Encryption |
|-----------------------------------|---------------------------------------|---|
| Online via Web(Browser) | Authentication via Login and Password | HTTPS (SSL) |
| Transaction-based via SMTP (Mail) | Authentication via Mail account | Optional but recommended via TLS or IPsec |
| Transaction-based via HTTPS POST | Authentication via Login, Password | HTTPS (SSL) |
| Transaction-based via HTTPS SOAP | Authentication via Login, Password | HTTPS (SSL) |
| Transaction-based via FTP | Authentication via Login, Password | SFTP (SSH) |

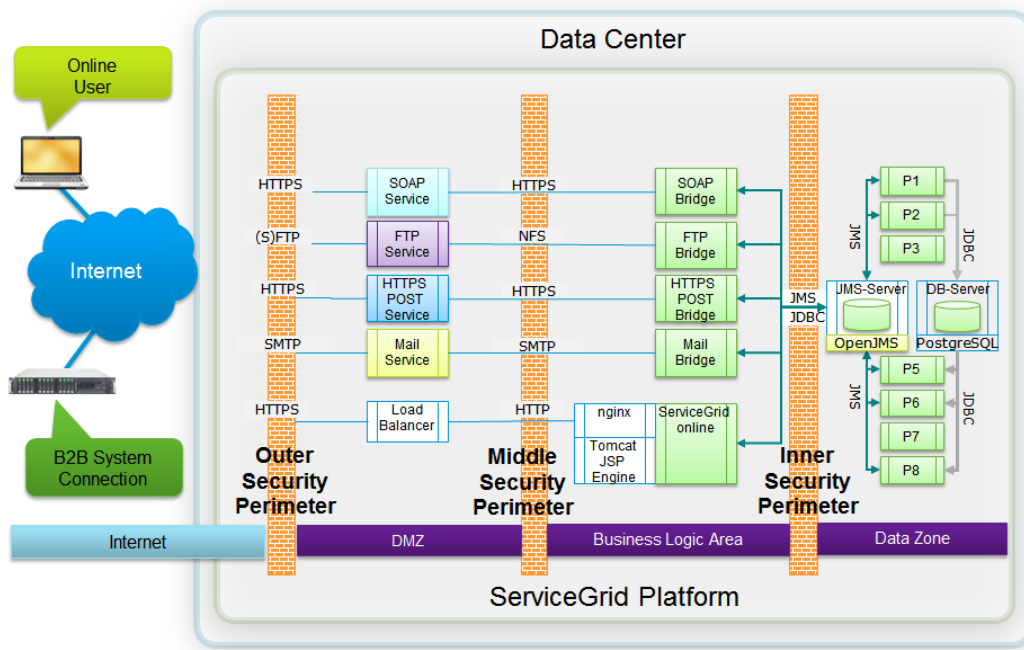


Figure 13. Services provided to ServiceGrid Users or connected Systems



2.7 Load Balancing and Clustering

For building high-availability and high-performance web applications, two main technologies are used:

- load balancing
- clustering (including replication)

Table 10: Load Balancing and Clustering

| | |
|-----------------------|---|
| Load Balancing | Load Balancing means that requests to a service are distributed to a number of servers which provide the same service. The main goal of load balancing is to increase performance, although it can also be used for high availability. |
| Clustering | Clustering means that a service is available on at least two servers, where in most cases one is "active" and the second is "passive", i.e. the second is in standby mode. |
| Failover | If there is a problem with the active node in a cluster, the passive server takes over; both servers change their active/passive roles. A passive node can be shut down and repaired any time. |
| Replication | Replication means that data is replicated to at least two nodes. Synchronous replication assures that every node will always deliver the same data. Asynchronous mode means, that there is one master and data is replicated to the slaves with some delay. |

Layers:

We distinguish between the following layers:

1. Hardware
2. Network
3. Application

Hardware Layer

There is no single point of failure in the hardware layer.

Every service cluster consists of at least two nodes. Every node uses a RAID mechanism to prevent data corruption, two power supplies to prevent unnecessary shutdowns and two network adapters to prevent network loss.

Network Layer

There is no single point of failure in the network layer.

Every physical server is connected to at least two network switches. If one switch fails, the other can handle all requests without any interruption. Every physical server has at least two network adapters, one for a redundant connection to another switch.



Application Layer

We need to distinguish between middleware software that needs to store shared data (e.g. a database server) and other software that just stores internal data or no data at all (e.g. Tomcat).

Database servers or Java Messaging Servers are operated in a synchronized cluster (using DRBD). This assures that if there is a problem on the hardware level, a failover is executed and the service is continued on the second node.

Load Balancing

Some services can be load balanced. Especially if they do not store shared data and operate stateless (e.g. SOAP servers). The load balancer distributes requests to a number of servers which provide the same service.

Load balancers not only help to improve performance, but can also provide high availability. If one of the load balanced servers fails, it is taken out of the load balancing and the remaining servers will handle the requests.

2.8 Scalability of Infrastructure

Scalability of the ServiceGrid platforms is a major design objective of the application and infrastructure architecture. Sizing of the platforms infrastructure is an ongoing procedure following the growth rates of the load.

2.8.1 Essential System Parameters

The essential system parameters are the basic indicators for calculation of the required capacity.

Table 11: System Parameters

| Parameter | Affected System Components |
|---|--|
| Number of concurrent online Users | Generates load for the application servers and to the data base server. Compared to B2B transactions the load generated by concurrent online users is approximately 50 times higher. |
| Number of service calls created | Generates load for the application servers and to the data base server. |
| Number of service call updates (history records) | Generates load for the application servers and to the data base server. |
| Number of B2B transactions per minute/second | Generates load for the B2B connections. |
| Number of data base transactions per minute/second | Generates load for the data base engine and data base server cluster. |



2.8.2 Essential System Components and Sizing Options

Application Servers

Application servers are operated in parallel. The load balancing process distributes the load to the application server array. Sizing is done by adding additional application servers and by upgrading memory and processor capacity.

B2B Connection Processing Cluster

The B2B connection Processing Cluster is dedicated to the converter processes. Sizing is done by adding additional clusters and by upgrading memory and processor capacity.

Data Base Server

The data base server cluster has to process all data base requests. For performance reasons the data base server cluster is a multi-processor architecture and is equipped with enough memory space to hold the complete database in memory. Sizing is done through memory expansion and upgrading to more processor capacity.

2.8.3 Monitored Values and Reference Profiles

The ServiceGrid Team is managing all public and private platforms. All these platforms are monitored and trend analysis is performed frequently. The trend analysis covers the process and server capacity values (load, response time, memory load, processor load) as well as the application load profile (number of concurrent users, number of transactions, number of messages, number of calls and call updates).

Using these figures and analyzing the historical trend, the capacity needs and the upgrading measures are decided. (See also "Capacity Management Process").



3 Technical Operation

3.1 Tools and Methods Used

The ServiceGrid team is using three different and independent systems for managing the ServiceGrid platforms:

- The CCC (Cloud Control Center) is used for managing the releases and software distribution to all ServiceGrid platforms.
- Opsview is used for monitoring host and process conditions and for alerting
- Extmon is used for monitoring the availability of platforms and services. (See Figure 14)

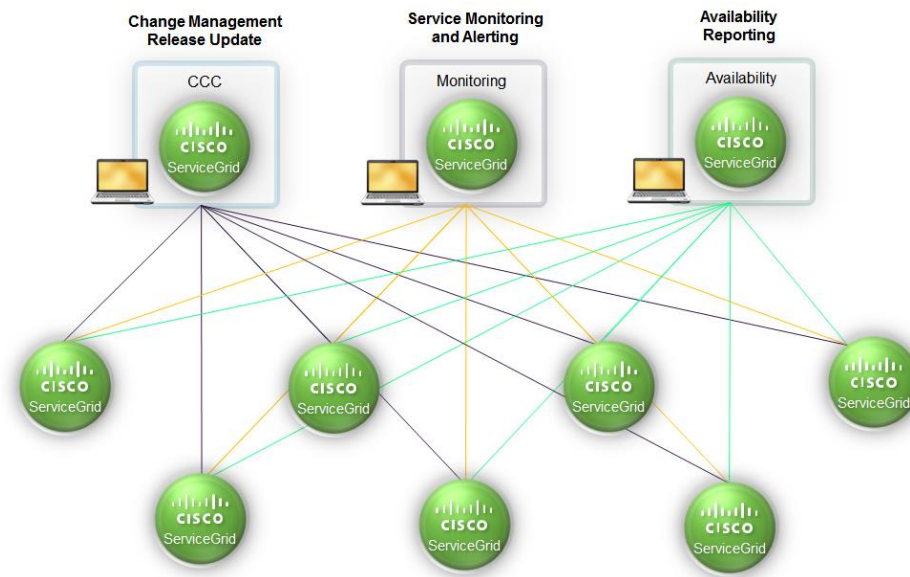


Figure 14. Tools for Managing the ServiceGrid platforms

3.2 Cloud Control Center (CCC)

All ServiceGrid platforms are permanently connected to the Control Center which is used to manage the ServiceGrid services by our Support and Technical Operations staff. The CCC is an essential part of the installation; it keeps the operating systems configuration up to date and synchronized throughout the whole platform. CCC is also used to deploy ServiceGrid release updates in a semi-automated way to minimize service downtime.

3.2.1 Technology Used

- The system monitoring is executed by the Technical Operations Team.
- The system parameters are monitored via Opsview using NRPE.



- The reporting is implemented by the ServiceGrid team, using a Round Robin database (RRD) and a reporting layer.
- Agents are implemented for server, network equipment, power switches and processes conditions.

3.3 Monitoring and Alerting

3.3.1 Objectives

A large number of system and process conditions are permanently monitored. The technical monitoring is described in the section “Technical Infrastructure”.

The monitoring follows two targets:

- Detection of error conditions: In case of critical conditions an automatic alert is created and dispatched to the ServiceGrid Operator on Duty (24/7).
- Provide data for trend analysis for capacity management: A selection of system conditions and values is collected in a RRD and provided for periodically analysis.

Availability Reporting: A monthly availability report for each ServiceGrid operating platform is available for ServiceGrid customers. (See section “Availability Management”)

3.3.2 Technology Used

All ServiceGrid Servers and Services are monitored 24/7 using Opsview. Every platform is connected via an IPsec tunnel to the monitoring infrastructure located in Vienna which enables the communication between the master and platform specific monitoring slaves.

3.3.3 Infrastructure Monitoring

The ServiceGrid team monitors the status of all servers using Opsview. Opsview servers try to connect to the Opsview clients on these hosts.

Besides the ServiceGrid application, a lot of additional health indicators are monitored. For instance, CPU load, temperature of the servers, disk space, RAID controller, fans, and more.

3.3.4 Application and Process Monitoring

All ServiceGrid processes write “Is Alive Files” every 30 seconds.

The Opsview client reads those “Is Alive Files” in a certain interval. If the file is older than the defined amount of minutes, the check will enter the warning level. If the file is older than the defined amount of minutes, the check will enter critical level.

The values for warning and critical differ and depend on the needs of the service and service level.



3.3.5 Alerting

Whenever the monitoring system encounters a critical error on a production platform, a short text message is sent to the technical operations team. This procedure is repeated every 30 minutes till the problem is resolved. Critical errors on TEST systems do alert only via email and have a lower priority.

Alerting and Escalation Procedure

- immediate notification is sent to the Support on Duty by text message
- Support on Duty is reachable 7x24x365

3.3.6 Tactical Monitoring and Strategic Monitoring

The central monitoring cluster collects all data from the different platforms or host groups.

Monitoring portals are implemented for:

- Tactical Monitoring
- Strategic Monitoring

The monitoring reporting interface is accessible by ServiceGrid technicians only. The monitoring functions are used by Availability Management and Capacity Management.

3.3.7 Tactical Monitoring

3.3.7.1 Using Opsview

The tactical monitoring and alerting is based on Nagios. The Nagios reporting interface is accessible by ServiceGrid technicians only. The monitoring functions are used by Availability Management and Capacity Management. (See Figure 15)

The screenshot shows the Opsview interface with a navigation menu at the top: STATUS, ALERTS, MODULES, HISTORY, CONFIGURATION, ADVANCED, SERVER, HELP. Below the menu, the breadcrumb path is 'Host Summary > Opsview > sdcall'. The main content is a table with the following structure:

| Host | Host Status | | Service Status Totals | |
|-------------------|-------------|-----------|-----------------------|-----------|
| | Handled | Unhandled | Handled | Unhandled |
| archive.sdcall | UP | | 4 OK | |
| archive01.sdcall | UP | | 15 OK | |
| archive02.sdcall | UP | | 14 OK | |
| backup.sdcall | UP | | 1 OK | |
| backup01.sdcall | UP | | 20 OK | |
| backup02.sdcall | UP | | 19 OK | |
| db.sdcall | UP | | 9 OK | |
| db01.sdcall | UP | | 20 OK | |
| db02.sdcall | UP | | 20 OK | |
| ettsbridge.sdcall | UP | | 3 OK | |
| filebridge.sdcall | UP | | 2 OK | |

Figure 15. Sample Opsview Screen



3.3.8 Strategic Monitoring / Reporting

3.3.8.1 Round Robin Data Base

Reports showing the time line of various values are implemented on base of a RRD. The RRD reporting interface is accessible by ServiceGrid technicians only (See section “**Security**”). The monitoring functions are used by **Availability Management** and **Capacity Management**. (See Figure 16)

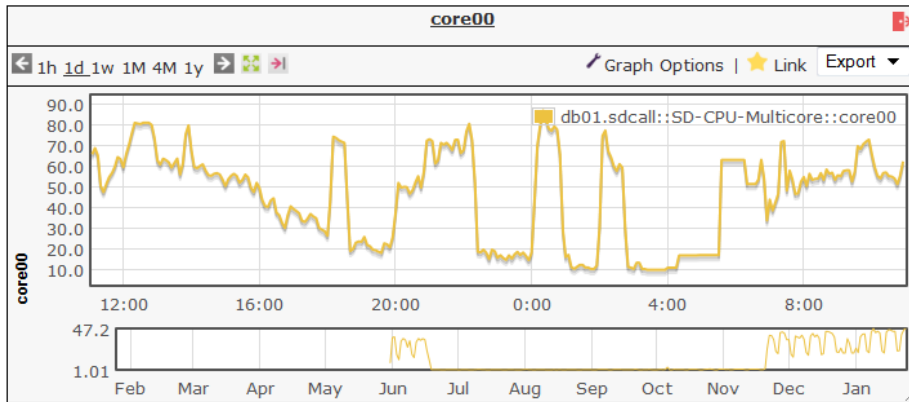


Figure 16. Sample Time Line (CPU Usage)

3.4 Availability Reporting

3.4.1 Technology Used

ServiceGrid uses 3rd party services for availability reporting like Pingdom, etc. All collected data is aggregated in the ServiceGrid “extmon” application and available for review. Figure 17 below shows an example of an extmon report. All data are shown in a user-friendly view.

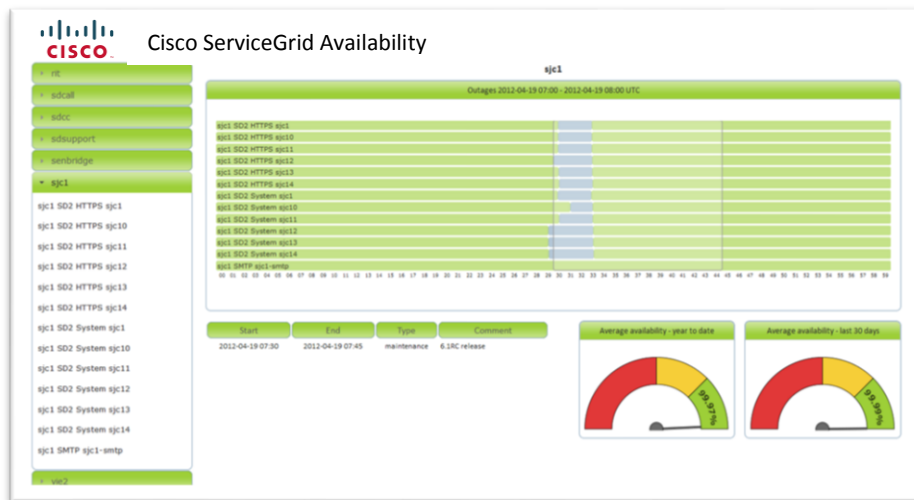


Figure 17. Sample extmon report



3.5 Capacity, Availability, Continuity

3.5.1 Possible Outage Scenarios

One hard disc defect

- Redundant Array of Independent Disks (RAID) system – just change the disc
- No outage

One server or RAID system defect / down

- Data replicated with a Distributed Replicated Block Device (DRBD)
- Second cluster node takes over
- Outage a few minutes

Data corruption on DRBD or both database (DB) servers lost

- Worst case scenario
- Point in time recovery with snapshot backup and Write Ahead Log (WAL) files
- Example: rollback release
- Outage: a few hours

3.5.2 Redundant Infrastructure

The ServiceGrid server and network infrastructure is based on redundancy.

Clusters

The mission critical processes run on cluster systems. A cluster consists of two complete redundant servers, bundled in a cluster via **DRDB**.

One of the two servers is always the primary node. Writes to the **primary** node are transferred to the lower-level block device and simultaneously propagated to the **secondary** node. The secondary node then transfers data to its corresponding lower-level block device. All read I/O is performed locally.

Should the primary node fail, a cluster management process automatically promotes the secondary node to a primary state (fail over).

Multi Server and Load Balancing

The capacity critical processes (Web Frontend processes) run on two or more parallel servers. A load balancing function distributes the incoming service requests to the servers. If a server fails or has reached its maximal load the requests are automatically routed to one of the other servers.



3.5.3 Data Backup

Data Base

Data backups from the platforms are automatically performed in a two-step procedure, following a multi generation principle.

For each ServiceGrid production platform in a data center the following data base backups are executed automatically:

- Daily Data Base (file) backup from the Data Base Cluster to the platform Backup Cluster
- Daily Data Base (file) backup from the platform Backup Cluster to a server in a remote location.
- Continuously Data Base WAL backup from the Data Base Cluster to the platform Backup Cluster

Data base backups are organized and stored in 7 generations.

3.5.3.1 Data Base Dump

- Starts daily after local business hours
- Dump saved on backup server
- Last seven dumps kept on backup server
- Copied every second day to a remote location

3.5.3.2 Point in Time Recovery

- Recovery to any time in the past 24 hours possible
- Backup of database directory four times a day to the backup server
- Archive WAL files all the day – every few minutes
- WAL files immediately moved to the backup server using rsnapshot
- Needed parts:
 - Binary copy of database filesystem (rsnapshot)
 - Permanent WAL file archiving activated
 - Everything triggered on the db sever – backup server only passive



3.5.4 Recovery

Backup Recovery Plan

Backup Recovery Plans exist for the following scenarios:

- Failure of a single server
- Loss or damage of the data base
- Loss or damage of configuration data
- Loss or damage of application files
- Complete loss of a data center

The Backup and Recovery Plans are managed by the Continuity Management Process.

Disaster Recovery Plans

A crisis plan is in place. The crisis plan covers the initial actions when a (possible) crisis is detected to form the Crisis Management Team in short time. The action plans and scheduled checkpoints are predefined as well as the internal and external communication streams. The crisis plan lists also the various Recovery Plans to be applied.



4 Security

4.1 ServiceGrid Platform

4.1.1 Defense

To protect the ServiceGrid platform against external attacks and to avoid intrusion through hackers, a segmentation into “zones” bordered by “perimeters” is implemented.

The complete network layout for the ServiceGrid application is based on the following structure:

- (External) Internet Zone
- ServiceGrid Outer Security Perimeter
- ServiceGrid DMZ : Frontend Services
- ServiceGrid Middle Security Perimeter
- ServiceGrid Business Logic Area
- ServiceGrid Inner Security Perimeter
- ServiceGrid Data Zone

A detailed network plan or list of the infrastructure (services and communications) is confidential and cannot be part of this document. The Technical Operations team maintains the appropriate information.

4.1.1.1 Zones and Security Parameters

Connections, processes, applications and databases run in the following four zones separated by three security perimeters:

Internet

Internet is the publicly used area and common infrastructure. This area is the so called “red zone” as there is no specific security mechanism installed to protect and secure information passing on.

Outer Security Perimeter

The perimeter takes care that only those kinds of data have access to the demilitarized zone (DMZ), which are intended for the frontend processes. The security gateway is a dedicated firewall.

DMZ

Within the DMZ all necessary frontend processes of ServiceGrid are running to communicate with service customers and service providers. This area is also called “yellow zone”, as the Internet DMZ is zoned to the Internet via the “outer security perimeter”, which ensures that only data pass which are allowed to have access to the frontend server. The frontend processes are typically web services (HTTPS), mail services (SMTP) or file services (SFTP).



Middle Security Perimeter

This perimeter divides the DMZ (frontend processes) from the Business Logic area and ensures that only data traffic from the frontend processes is passed to the application server for further processing, and vice versa.

This security gateway is a dedicated firewall.

Business Logic Area

Located in the Business Logic Area are all processes necessary to implement the business logic for the frontend services. This concerns mainly the Application Server.

Inner Security Perimeter

This perimeter divides the DMZ (frontend processes) and the Business Logic area from the Data Zone (middleware) and ensures that only data traffic from the frontend processes, respectively the application server, is passed to the Data Zone for further processing, and vice versa.

This security gateway is a dedicated firewall.

Data Zone

The Data Zone runs the middleware (partially Java Message Service (JMS) server, content and customer data in databases), which has to be treated as a highly secure and highly confidential area.

This area is also called “green zone”, as the “middle security perimeter” ensures, that only the processes in the Business Logic Area have access to the application server and its data.

4.1.1.2 Firewalls

The firewalls for the different security perimeters are logical views of one physical firewall cluster. All parameters and settings are defined by the ServiceGrid team in collaboration with internal and external security experts. Only those IP addresses and ports are opened, which are absolutely necessary to access the appropriate services. All other addresses and ports are blocked. This guarantees a secure and reliable area to run the application on this platform.

4.1.1.3 Defense against Denial of Service (DOS) Attacks

ServiceGrid uses more ways to protect its systems from DoS attacks:

- All ServiceGrid systems placed in the Outer Security Perimeter and all systems which forward network traffic use a hardened GNU/Linux TCP/IP stack. This type of defense should prevent some packet [SYN, ...] flood attacks.
- To prevent attacks focused on HTTPS DoS, ServiceGrid uses a two-way load-balancing system which uses IP LVS [directord] which forwards the requests to two separate Load-balancers which use non-blocking I/O – nginx – which is extremely well performing. This HTTPS server is also not vulnerable to “Slow loris” type attacks. As back end servers Apache Tomcat application servers are used.



- Last but not least we monitor all connections and group them by network, which enables us to block particular traffic from a network after serious suspicion of a DoS attack.

4.1.2 Database Access

Data Zone

All data is stored in a relational database in the Data Zone. Connecting to the database management system (DBMS) is only possible with a valid user/password combination. Access is restricted to authorized users.

Database structure and company data

The data in the database is organized by company accounts. That means that each record in a table containing company-specific private data

- is referenced to the company (account).
- can only be viewed by an authorized user who is a member of the company account.

For details see section “Architecture”.

4.2 Connectivity

The connection to ServiceGrid is through encrypted connections and needs authentication:

Table 12: Connectivity

| 1. Access Method | 2. Authentication | 3. Encryption |
|--------------------------------------|---------------------------------------|------------------------------|
| Online via Web(Browser) | Authentication via Login and Password | HTTPS (SSL) |
| Transaction-based via SMTP (Mail) | Authentication via Mail account | Recommended via TLS or IPsec |
| Transaction-based via HTTPS POST | Authentication via Login, Password | HTTPS (SSL) |
| Transaction-based via HTTPS SOAP | Authentication via Login, Password | HTTPS (SSL) |
| Transaction-based via SFTP | Authentication via Login, Password | SFTP (SSH) |



4.2.1 Transaction Based B2B Data Exchange

ServiceGrid provides six standard communication types for transaction based communication as used with ServiceGrid connectors:

- SMTP
- SFTP
- HTTPS SOAP
- HTTPS POST

Depending on the communication type used as transport protocol, there are different possible options for security. In all cases the Internet protocol is used as network protocol. In terms of security, two options can be applied:

- **Internet via SSL**
The public internet provides a simple and commonly used standard to connect and to exchange data using TCP/IP. The communication partners are authenticated and the transferred data is encrypted using Secure Socket Layer (SSL). SSL is the underlying mechanism of HTTPS and SMTP (via TLS).
- **Connect over the Internet via IPsec**
As an alternative to the easy transport via internet, ServiceGrid provides the possibility of an IPsec connection. IPsec allows a secure and encrypted way of communication between service customers or service providers and ServiceGrid application. For more details about IPsec please see section below.

4.2.2 Online Access

4.2.2.1 Types of Users

Access to the ServiceGrid application and to the system layers is restricted to dedicated groups of users.

- **System Administrator:** any person with access to servers of the ServiceGrid main platform on operating system level.
- **Application Root Administrator:** any person with administrative access to all company accounts within the ServiceGrid platform.
- **Application Developers:** The application developers provide updates and new releases of the ServiceGrid application. Application developers are also responsible for 3rd level support in case of incidents or system malfunctions. Therefore application developers need a limited access on operating system level.
- **Application Administrator:** any person with administrative access to certain company accounts within the ServiceGrid platform.
- **End User:** any person who uses the ServiceGrid application via browser for his daily job (e.g. create calls) without doing any administrative tasks.



4.2.2.2 ServiceGrid Technicians

Persons involved in the administration and operation of the ServiceGrid main platform are defined as ServiceGrid Technicians. Roles include:

- **System Administrators** with root access to the servers
- **Application Developers** with limited system administration access to the servers
- **Application Administrators** with superuser access to the application (members of the ServiceGrid root account)
- The (first) **Application Administrator** of a ServiceGrid customer

Authorization

Each modification of user access rights on the platform (OS-level and application administration), which is subject to internal controls, needs the approval of the system owner. It must be assured, that the segregation of duties is taken into consideration.

1. The user's manager requests permission
2. The delivery manager grants the permission
3. An administrator (OS or application) implements the permission

4.2.2.3 Access to the System Layers

System Access for system administration tasks is allowed for ServiceGrid Technicians only.

System Access is allowed only from

- fixed known IP addresses of the technical operations team,
- the monitoring and web cluster for receiving monitoring data

From these IP addresses, access to the DMZ is allowed using the SSH service.

4.2.2.4 Access to the ServiceGrid Application

The interactive access to data and functions is implemented via HTTPS sessions. A login process is required to start the session. There is no other interactive access possible.

The complete list of URLs for the various ServiceGrid platforms is described in Appendix A.



4.2.2.5 Application Administrator Login

For application administrators the following measure is implemented additionally:

The first login date and the last login date is stored in the ServiceGrid application database and can be displayed as part of the user's basic data.

4.2.2.6 Application Login Procedure

Access to the ServiceGrid platform via Portal is only possible for authorized users. An authorized user is defined via a user record in the ServiceGrid database:

- Each user only has access to the company ("account") data of the company she/he is member of.
- Creation of new user records or disabling of users is managed and controlled by the company's administrator only.
- Membership and permissions (login, password) of users are managed and controlled by the company's administrator only.

The login process requires login name and password. The user has to enter login name and password. When the application is not used for a certain period of time (30 minutes), the session is automatically closed and the user has to login again. Passwords in the ServiceGrid database are encrypted, using an SHA-256 salted hash algorithm.

Application administrators can define IP ranges to restrict the access to the ServiceGrid application to defined networks for their company. If a user tries to log in and is member of an organization which has restricted access, the destination IP address is checked and the login is refused if the IP address does not match.

4.2.2.7 Password Policy for Customers

The password policy is controlled and managed by the company account administrator only. The password policy contains rules for format, content and the duration of validity of passwords:

- Minimum password length
- Maximum password length
- Maximum number of wrong password attempts
- Password history length
- Minimum password change interval in hours
- Password duration in days
- MustUse capitals
- MustUse digits



4.2.3 Encryption Using HTTPS (SSL)

HTTPS has to be used when

- accessing the platform as an interactive user
- using SOAP as a transport protocol
- when using HTTP POST as a transport protocol

In these cases, no other (weaker) encryption method is possible.

4.2.4 Tunneling via IPsec

As an alternative to the direct transport via SSL/TLS via Internet, ServiceGrid provides the possibility of an IPsec connection. IPsec allows a secure and encrypted way of communication between service customers or service providers and ServiceGrid application.

4.3 Environment, Data Centers

4.3.1 Scope

The ServiceGrid platform is installed and operated out of data centers implementing a secure environment.

- ServiceGrid has a collocation contract with the data center operator including the providing of space and connections to the internet.
- The ServiceGrid platform itself is operated by the ServiceGrid technical operation team.

4.3.2 Defense

The ServiceGrid platforms infrastructure (servers and local network components) are installed in rack mounted server boxes inside the data centers. The boxes are locked and can only be unlocked by the ServiceGrid operation team.

Security measures are provided by the data center operator:

- Personal access control, authorization mandatory
- Video surveillance
- Visitors escorted
- Fire extinguishing system

The security measures are part of the collocation contracts between Cisco and the data center operator.



4.4 Environment, Office

4.4.1 Scope

In scopes of this section are all employees and their computers, and the technical infrastructure of ServiceGrid, if involved in administration, maintenance or development of the ServiceGrid platforms or the ServiceGrid application.

4.4.2 Defense

Software development and technical operation activities are carried out in the Cisco office, Vienna, providing a secure environment.

Dedicated Firewalls

Dedicated firewalls are installed to protect the ServiceGrid lab network from the Internet. All the parameter settings are defined by Cisco Security in collaboration with external security experts. Only those IP addresses and ports are opened, which are absolutely necessary to access the appropriate services. All other addresses and ports are blocked.

Personal Access control

Access to the Cisco office follows a two stage access procedure:

- Access to the building is possible only via a reception desk or a badge.
- Access to the Cisco office within the building is only provided for authorized persons or guests and protected via the Cisco reception desk or a personal badge.
- Servers are installed in a dedicated locked lab environment. Access is restricted to authorized persons.
- Guests are always escorted.

4.4.2.1 Computer Malware Prevention

If malware is introduced to the Company IT network, data loss, corruption, or misuse of company computing resources or information may occur. All technically and economically justifiable actions need to be taken to prevent the introduction malware to the company IT network. The standard operating procedures are defined in the **Cisco internal security policies**.

4.4.2.2 Nondisclosure Agreement

All staff members of Cisco have signed a **Non-Disclosure Agreement** with their contract.



5 Data Privacy

5.1 ServiceGrid Application

The ServiceGrid application and the operating environment contain a number of organizational and technical measures designed and implemented to follow the rules and regulation for data privacy.

As ServiceGrid is a “Software as a Service” (SaaS) platform the application, infrastructure and technical operation of the platform is provided in a way that the ServiceGrid customer is able to fulfill the data privacy requirements specified by the country or region specific laws and regulations.

These laws and regulations could apply:

- European Union: Data Protection Directive (officially Directive 95/46/EC)
- Austria: Datenschutzgesetz
- Germany: Deutsches Bundesdatenschutzgesetz

Cisco is describing all technical and organizational measures helping to achieve full compliance to the regional laws and regulations. Due to the nature of a SaaS application regarding the data transported, processed and stored, Cisco cannot guarantee full compliance to data privacy laws and regulations for each usage of the ServiceGrid platform by ServiceGrid customers. It is in the responsibility of the ServiceGrid customer to organize the usage of the functions provided by Cisco in a compliant way.

5.1.1 Data Managed and Stored within the ServiceGrid Application

Cisco stores data provided by the ServiceGrid customers on the ServiceGrid platforms. This data may include personal data (e.g. name, address of persons). It is up to the ServiceGrid customer which personal information is stored on the ServiceGrid platform and data base. Cisco is not able and will not take responsibility for the content of data including personal data transported, stored and processed by the customer on the ServiceGrid platform.

5.1.2 Location of Platforms and Data

Cisco provides its shared ServiceGrid platforms either in EU (Austria) or US (California / Texas). The customer decides where his account and data is stored.

In the case the customer is using more than one platform it's up to the customer to decide which data is stored on which of the platforms following the technical options and restriction of the ServiceGrid application.

Transport of data between two or more ServiceGrid platforms is restricted to service case transactions and thus also restricted to the data and personal information in those transactions. The data structure used for these transactions is defined and provided as specification to the customer. It is in the responsibility of the customer to decide which data and personal information may be included in this transactional data.

In case the customer decides to run ServiceGrid within it's own premises (private cloud) the customer decides and takes responsibility for the location of data



5.1.3 Secure Transport of Data

Transport of data to and from the ServiceGrid platforms is protected by the Cisco security policy and the technical and organizational measures.

These measures include: encrypted transport based on SSL, VPN tunneling as an option, authentication methods as defined by the specific transport protocol.

5.1.4 Secure Access to Data and Functions

Processing and storage of data on the ServiceGrid platform is protected by the Cisco security policy and the technical and organizational measures. This includes: encrypted online access security perimeters to protect data stored, secure access to the datacenter, and many more

Password policy is selectable by the customer.

5.1.5 Secure Storage of Data

The ServiceGrid platforms are operated on a redundant infrastructure based on clusters and load balancing to multiple application servers.

Data backup is automatically performed to a backup server within the data center and to a remote location in the same region.

5.1.6 Access and Usage of Data

The ServiceGrid technical team has access to the ServiceGrid platforms and data for maintenance and support reasons.

Cisco will not use the customers' data for other reasons than maintenance and/or support tasks. Furthermore Cisco is strictly committed to handle all customer data and information stored by the customer on the ServiceGrid platforms as strictly confidential.

The list of Cisco employees having access to customer data is restricted to ServiceGrid team members of the technical operation, development, support and project consultants. All employees have signed a non-disclosure agreement.

The technical access to the ServiceGrid platforms for Cisco employees is either through the defined online access as used by the customers and protected in the same way, or through the system maintenance access restricted to defined IP addresses within the Cisco internal network.



5.1.7 Update of Change of Customer Data

Cisco will change, update, delete or insert customer data on the ServiceGrid platform only on written instruction from the customer. This is the case when performing support tasks for the customer and/or during service projects ordered by the customer.

5.1.8 Deletion or Anonymizing of Data

ServiceGrid provides functions for anonymizing data. These functions are designed to overwrite personal data (e.g. names, addresses) following the specific data privacy rules obeyed by the customer.

ServiceGrid will not execute data anonymizing automatically. Responsibility to trigger data anonymization is with the customer. ServiceGrid will run data anonymization procedures only on written instruction by the customer.



6 Internal Control System

The Internal Control System (ICS) of the organization is designed to help the organization accomplish specific goals or objectives. It is a means by which an organization's resources are directed, monitored, and measured. The ICS consists of a set of internal Controls, called the control set.

6.1 Environment

Management Commitment

The general corporate policy defines the high level business and quality goals and confirms the management commitment to these goals. The individual goals for the various organizational units and processes are derived from the general corporate goals.

Quality Management

Quality management means the systematic way of ensuring that all activities necessary to design, implement and deliver services which satisfy the requirements of the customers take place as planned and that activities are carried out cost effectively. The way this is achieved as specified in the ICS defining the responsibilities, policies, processes and standard operating procedures required to deliver high quality services.

Segregation of Duty

Segregation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users.

6.2 External Assumptions at Client Side

The internal controls are designed and implemented following the assumption that certain controls and responsibilities are implemented on the side of clients having contracted services with Cisco. Controls and responsibilities include:

Security:

The customer application administrator is responsible for granting access permissions for the users on the customer side. The customer administrator is responsible for setting the password policy.

Project Implementation:

The project manager on the customer side is responsible for the acceptance procedure.

Incident Management:

The customer administrator is responsible for reporting incidents to the Cisco TAC Support.



6.3 Monitoring

Service Case Monitoring

For operations, all relevant processes are structured according to ITIL and defined comprehensively in the internal process documentation. A control framework is defined using the COBIT model and integrated in the process descriptions. As far as possible, the controls are followed-up by service case tickets. The tickets are also used for documenting the result of the individual control activity.

The performance indicators of the various service cases are monitored and reported in the internal service management support account. Service case tickets are generated for:

- Infrastructure alerts
- Incidents
- Problems
- Application changes
- Infrastructure changes
- Releases

For each of this type of service cases the following performance indicators are monitored:

- Volume by period
- Open/Closed cases
- Service level fulfillment
- Response time
- Recovery time

Technical Monitoring

The technical monitoring of the operation infrastructure and all supported systems is described in detail in the section “Technical Infrastructure” of this report.

6.4 Structure and Framework

Cisco ServiceGrid has defined and implemented a COBIT Control based ICS. This helps to steer or navigate the process to goals and objectives.

Each control consists of:

- Control Objective (What is important?), e.g.: *Controls provide reasonable assurance that incidents are detected, communicated, documented and resolved in a timely manner.*
- Control ID, eg INC-04



- Control Description (What to do?), eg: *All incidents are closed after they have been solved. The solution is documented in a mandatory field in the ticket and communicated to the customers.*
- Control Detail (How?) ,eg: *Incident Management Tasks* (See Figure 18)

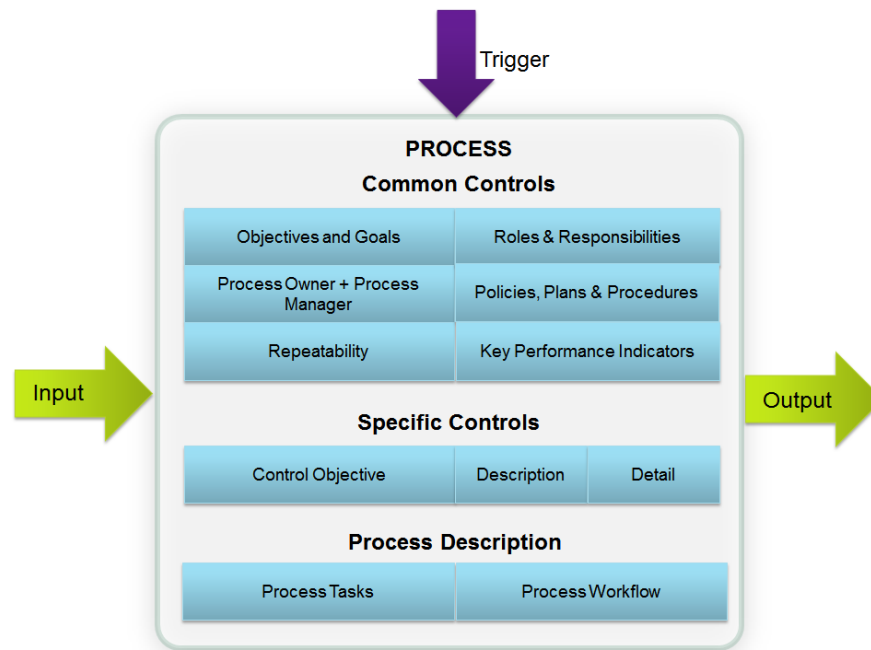


Figure 18. Common Controls

The internal controls are defined and implemented within processes covering the areas of service delivery and service support. A process describes the act of taking something through an established and usually routine set of procedures.



7 Appendix

7.1 URLs and Services

The ServiceGrid application is accessible via those URLs and provides those services:

| SDCall Platform | |
|---|--|
| https://sdcall-portal.solvedirect.com | .. ServiceGrid Web Application |
| https://sdcall.solvedirect.com | .. Legacy ServiceGrid Web Application |
| https://mobile.solvedirect.com | .. Mobile version of the ServiceGrid Web Application |
| https://ws.solvedirect.com | .. WebServices (SOAP) and HTTPS POST |

| VIE2 Platform | |
|---|--|
| https://vie2-portal.solvedirect.com | .. ServiceGrid Web Application |
| https://vie2.solvedirect.com | .. Legacy ServiceGrid Web Application |
| https://vie2-mobile.solvedirect.com | .. Mobile version of the ServiceGrid Web Application |
| https://vie2-ws.solvedirect.com | .. WebServices (SOAP) and HTTPS POST |

| SJC1 Platform | |
|---|--|
| https://sjc1-portal.solvedirect.com | .. ServiceGrid Web Application |
| https://sjc1.solvedirect.com | .. Legacy ServiceGrid Web Application |
| https://sjc1-mobile.solvedirect.com | .. Mobile version of the ServiceGrid Web Application |
| https://sjc1-ws.solvedirect.com | .. WebServices (SOAP) and HTTPS POST |



7.2 Private Platform Configuration

The following list describes the recommended hardware components to operate the ServiceGrid application in a private cloud, based on Cisco hardware. It is a recommendation for a small to medium size platform and will be able to handle 400 concurrent users and 2 million transactions per year.

| Count | Configuration | Purpose |
|-------|--|---|
| 2x | ASA5545 | Firewall Cluster |
| 2x | UCS C240 2x Xeon E5-2609, 16 GB RAM, 8x 1 TB SAS, Raid 5 | Backup Cluster |
| 3x | UCS C220 2x Xeon E5-2609, 16 GB RAM, 2x 120 GB SSD, Raid 1 | DMZ, Load balancer Cluster, Front End Cluster |
| 4x | UCS C240: 2x Xeon E5-2643 v2, 256 GB RAM, 4x 600 GB SAS, Raid 10 | Database Cluster, File Storage Cluster, Process Cluster |
| 3x | UCS C220: 2x Xeon E5-2643 v2, 128 GB RAM, 2x 120 GB SSD, Raid 1 | Bridge Cluster, Application Servers |
| 1x | CISCO3945/K9 | Management Console Access Router |
| 2x | UCS C240: 2x Xeon E5-2643 v2, 256 GB RAM, 4x 600 GB SAS, Raid 10 | Reporting DB (Optional) |
| 3x | UCS C240: 2x Xeon E5-2643 v2, 256 GB RAM, 4x 600 GB SAS, Raid 10 | ActiveSLA (Optional) |



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)