overcast

Overcast Security White Paper

Januar 2023

Introduction

Overcast is a Salesforce-native cloud integration service that lets you quickly and easily connect Salesforce to on-premise or other cloud-based systems. Interconnecting and integrating different cloud and/or on-premise information systems demands first-class security to protect the connected and integrated systems and their data.

Security must not be an afterthought, but instead, Vigience designed Overcast with security in mind from the bottom up. Security policies are well observed at Vigience and followed throughout our Software development process as well as in our daily operations.

The various aspects of security regarding Overcast as the software and Vigience as the vendor and operator of the solution are described in this security white paper.

The information in this paper is based on release v2.90+ of Overcast. After an introduction to the Overcast architecture, this paper will detail in the following sections how security addressed regarding storage, access control, data transmission, deployment and operations, and the software itself. Finally, the last section covers the subjects audit and certifications.

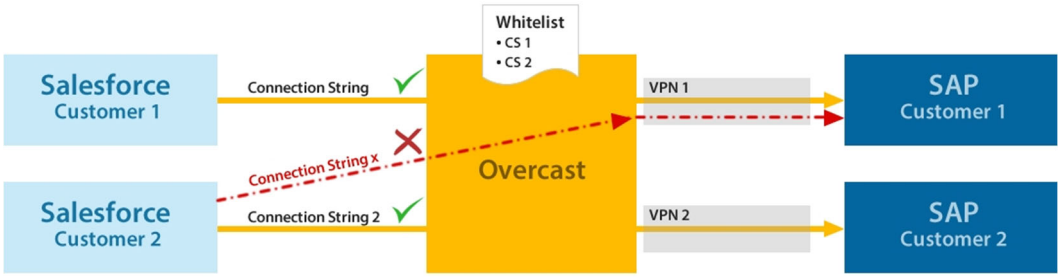
Overcast Architecture

To describe the security concepts around Overcast, it is necessary to first have a look at the overall architecture and describe the main components. The Overcast Service Endpoints residing in the cloud, running on the Microsoft Azure platform, deal ~~mainly~~ with the connection handling of the customers' backend systems and bridging the protocols that are supported by the backend to a web service that can be consumed by Salesforce. These server components are written in .Net. The following diagram shows the high level Overcast architecture:

- Overcast is installed in the Salesforce org of the customer via a managed package from the Salesforce AppExchange.
- Overcast can access backend systems via different protocols and formats like RFC, OData, SOAP and REST web services etc. through the Overcast Endpoints. These endpoints are a cloud-based service hosted by Vigience on the Microsoft Azure platform and they enable the connections to the backend systems and bridge protocols.
- The connection to the customers backend systems in the cloud or on premise can be established either via VPN or via the Overcast Secure Agent.

Workspace Concept for Multi-tenancy

Multi-tenancy is a necessary property of all cloud solutions used in a business context. It enables the separation of data from different customers, even though all customers are using the same system and infrastructure services. Overcast achieves multi-tenancy by being installed in the customers Salesforce Org. This org, which is under full control of the customer, holds all relevant information regarding connected system information, credentials and business data like accounts and products. The Overcast Whitelisting concept ensures that customers can only access their own backend systems.



Secure Data Storage and Data Encryption (Data at Rest)

Overcast Endpoint

The Overcast service in the cloud is the endpoint for the secure connection from Salesforce to the customer's backend systems. It bridges different backend protocols and transforms data formats so that they can be consumed by Salesforce. The Overcast endpoints are stateless and do not make use of any persistent storage or databases and therefore do not store any data, i.e. neither customer information like business data nor any other sensitive information like usernames or passwords. Since Overcast endpoints are stateless, there is not data residency on the overcast endpoints and data-at-rest encryption is not applicable.

Salesforce

Overcast stores the following information within Salesforce:

- Business Data replicated from the customers backend systems.
- Connection information like server names, ports etc.
- Sensitive information like username/password (always encrypted). The encryption key is generated, but not stored, on the Overcast endpoint. It will be saved within the Overcast managed package as a protected custom metadata type. Neither Vigience nor the customer has access to it. It can only be used by the manged package itself to encrypt and decrypt the sensitive information.

Business data can be encrypted within Salesforce if required to comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

Data that is fetched from a customer's backend system via a real-time integration is not permanently persisted within Salesforce. It is only available in memory to display it to the user, and it is removed afterwards.

Access Control

Access control lists are used to restrict access to authorized endpoints/systems only. Secure agent connections are established against Salesforce using OAuth.

End User Authentication

Overcast is installed in Salesforce as a managed package. End users, as well as system administrators and developers log in via the standard Salesforce UI. Salesforce offers role-based access controls (RBAC) to provide access to its platform. With that, access to Overcast itself, but also to components developed with Overcast, can be restricted.

A technical user is used by Overcast to connect to backend systems. This ensures that the backend controls what type of access is granted.

In some cases, it is necessary to implement a user mapping between the backend user and the Salesforce user to execute transactions in the context of an individual user and with the authorizations of this user.

Limit access to sensitive data

Access to business data can be restricted by standard Salesforce concepts like roles, profiles and permission sets.

Vigience internal

The staff at Vigience itself follows strict security policies. Background checks on prospective new recruits are an essential part throughout our hiring process.

Information related to any of our systems is only shared on a need-to-know basis. Only a small, selected group of users have access to production systems. Access is monitored and audited.

As stated in the Overcast Master Service Agreement, Vigience is maintaining appropriate administrative, physical, and technical safeguards for protection of the availability, confidentiality, and integrity of all our systems.

Network Security (Data in Motion)

All data transmissions are secured using TLS with certificates issued by a well-known certificate authority, Sectigo (https://sectigo.com). Our servers are configured to always use HTTPS/TLS. We configure them to use the latest TLS protocols and cipher suites and remove deprecated protocols and cipher suites from use. The following describes the current HTTPS configuration our server's use.

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

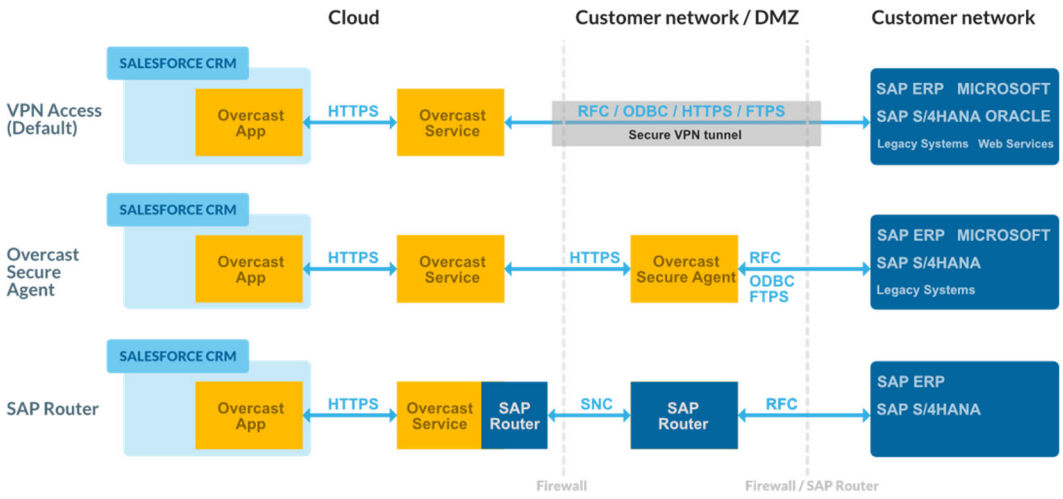
Cipher Suites

# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128

All requests to the Overcast servers are signed using an org-specific private key and verified by the corresponding public key on the server. The org's private key is secured in the Salesforce package in a protected custom metadata type.

On-premise systems which provide an internet-accessible API (e.g. SOAP or REST web

service) can be accessed by Overcast directly. On-premise systems that are not exposed to the public internet can be connected to Overcast via three different ways, that are illustrated in the following diagram:



Connection Options

Site-to-Site VPN

A site-to-site VPN connection is established via the Overcast endpoint and the customer's network. The following VPN configuration options are supported:

- VPN Type:
  - IKE Versions: IKEv2
  - Tunnel Type: Route-based
- Phase 1 (IKE) Parameters:
  - Encryption: AES 256 CBC, AES 256 GCM
  - Integrity: SHA 256, SHA 384
  - DH Group: 14 (MODP 2048)
- Phase 2 (IPSec) Parameters:
  - Encryption: AES 256 CBC, AES 256 GCM
  - Integrity: SHA 256, SHA 256 GCM
  - DH Group: 14 (MODP 2048)

A site-to-site VPN connection allows all connection types (i.e. backend protocols) supported by Overcast.

Overcast SecureAgent

The Secure Agent currently supports connecting to the following backend systems:

- SAP (RFC/Netweaver stack)
- SAP HANA
- MS SQL Server
- OData
- CSV files via FTP or network shares.

It must be installed on a windows server within the same network as the customers backend systems.

SAP Router

In this scenario, the SAP Router on the customer site and the one on the Overcast endpoint will be configured to communicate with each other. The connection is via the Network Interface (NI), which is used by SAP for remote function calls. The NI protocol uses TCP or UDP. The protocol is also known as the SAP protocol.

Deployment and Operations

Our servers are firewalled at both the data center infrastructure level, as well as the operating system level. We firewall off all ports other than the HTTPS 443 port. On our client-dedicated deployments, additional whitelisting is applied for known domains.

Regular monthly maintenance is scheduled to coincide with the Microsoft security updates.

Administration access to Overcast servers is only through VPN and secure locations whitelisted in the firewall.

Software

The software is digitally signed by Vigience and verified by the OS to assure that the code has not been tampered with. Patches for publicly disclosed vulnerabilities in the software stack are applied when made available by the vendors. To avoid security holes in the software, the development process follows industry best practices, including code and architecture reviews, threat analysis workshops and thorough security testing.

In addition to code review done by developers and architects, automated code analysis tools are employed to eliminate coding mistakes. Regarding testing, standard tools from Microsoft are used to guard against potential vulnerabilities that could be exploited by an attacker.

Audits

All process requests are logged and can be traced back into what API was used, by whom and when in the case of suspicious or suspected malicious access. These logs are stored in the customers Salesforce org.

Certifications

ISO27001-27017

ISO 27001 is the leading international standard focused on information security. It was published by the International Organization for Standardization (ISO), in partnership with the International Electrotechnical Commission (IEC). Both are leading international organizations that develop international standards.
ISO 27017 is a security standard developed for cloud service providers and users to make a safer cloud-based environment and reduce the risk of security problems.

Vigience is ISO27001 and ISO27017 certified.

Salesforce Certification

Overcast is available as managed package in the Salesforce AppExchange. In order to be available in the AppExchange, Overcast went through a security audit and test by Salesforce.

SAP Certification

Overcast is certified by SAP for use with SAP ECC 6.0/ERP and S/4HANA.

Conclusion

As has been outlined above, Overcast is a secure platform for integrating Salesforce with backend systems. Security measures are in place and have been reviewed to guard the confidentiality, integrity, and availability of information. Security is addressed on all levels: Secure data storage, access control, security in transit, deployment and operations as well as the software itself. Audits are also possible.
The Overcast platform is therefore well suited also to be used in enterprise environments. Its advantages and features make it an ideal tool to integrate Salesforce with systems like

SAP ERP, SAP Business One, Microsoft Dynamics, web services and others. Companies can trust that their data will not be compromised.

About Vigience

Vigience is a specialized Salesforce ISV partner that enables advanced, highly connected Salesforce solutions. We provide “true real-time connectivity” between Salesforce and any on-premise systems-of-records (SOR). We believe that the state-of-the-art enterprise software architecture in the coming decades will consist of the Salesforce platform as a dynamic system-of-engagement (SOE) on top of SAP S/4HANA as the system-of-record that powers all key business processes. We further believe that one can only empower people to work and interact in new ways when frontend applications like Salesforce are deeply integrated with core backend processes and data. To make that all possible, Vigience develops, implements, and distributes its unique product called Overcast.