



**OSvC TECHNICAL SUPPORT**

**WEBINARS:**

**OSvC Networking Best Practices**

*• our experts, your guides •*

**Cameron King, CCNA**

**OSvC Environment and SSL/TLS Support**

**September 12, 2018**

# Overview

Webinar will be presented in a server-end to client-end format, meaning we will start the discussion with how your site is hosted from the perspective of Oracle's infrastructure, to how it interacts over the Internet, and finally to the client device connecting to us. The aim is to keep the networking principles simple and easy to follow. Some of the following major topics will be discussed:

- **Oracle infrastructure, data centers, and servers**
- **Domains pertinent to OSvC vs external services that connect to your site such as third-party add-ons**
- **Bandwidth Requirements**
- **Firewalls, proxies, VPNs, and other access control**
- **Usage of custom domains**
- **Key networking differences between chat and the primary service module of the application**

# Oracle Infrastructure Basics

- Oracle has data centers around the globe, mostly in major metropolitan regions, Virginia, Chicago, Sydney, London, etc. We usually denote these shorthand as in VA, MW, SY, GB, and refer to them as pods.
- Sites are hosted in virtualized server clusters, operating from a pool of resources local to the data center. It is a shared multi-tenant environment which allows us to scale to client needs.

# Oracle Infrastructure Basics, continued

- All functions related to a site are hosted in the client's respective pod. If their site is in VA for instance, the mail servers, utility servers, file attachment servers, database servers, are all located in this data center. When you connect to your site you are effectively connecting to a single geographic location
- Servers in our infrastructure are referred to as "vips" (virtual IP/virtual host), and use the \*.rightnowtech.com domain format. These are logically and numerically named based on their functions (dbva01, fattachva01, filterva01, so if they appear in logging you can often get a sense of what their function is just by looking at the hostname.

# Oracle Infrastructure Basics, continued

- Nearly all of the traffic you see from your end will be to your primary vhost/primary vip, and your chat server if applicable. Everything in the database tier will be to your primary vhost, whereas chat traffic will be to the chat server.
- The primary vhost is the final landing page for your end-user page traffic, and what is shown in the browser when a user navigates to your page. When your site is newly provisioned, it will use our \*.custhelp.com wildcard cert and domain, so that it can use SSL/TLS to encrypt traffic. You can provide us with your own server certificate for SSL which allows you to use your own domain for an interface

# Considerations over the open Internet

- Your site uses standard web traffic ports 80 and 443, and in many ways functions just like any other web server you find on the Internet. In general, we do not perform whitelisting or blacklisting on our end unless there is a specific reason to do so, such as in the case of known malicious activity. Otherwise, our services are designed to be available on the web at all times, and we allow you to perform your own access control.
- The only real exception to this concept comes in with custom integrations. Oracle has in-house customizations support but also allows you to connect to an API, so that you can have your own developers write customized code. These tools will frequently have separate networking requirements, and need to be distinguished from ordinary OSvC traffic for this reason.

# Considerations over the Internet – Proxies

- For the very best performance available, we always recommend to clients that they try to reach us over the open Internet as much as possible, limiting interfering devices such as proxies.
- You can obtain the greatest overall speed by encouraging the user's device to bypass proxies, or have these network appliances contain exclusions for Oracle Service Cloud traffic and domains.
- Much of this is due to the primary function of proxies, which is to weigh in on every network communication to authenticate first. When dealing with the above-average volume of traffic produced by Oracle Service Cloud due to its complexity, and how many agents you may have using it simultaneously, this design can severely hinder performance and the user experience.

# Considerations over the Internet - VPNs

- Most major enterprise networks use some combination of proxies and VPNs, largely for their inherent value to network security. They are excellent for this purpose, but one should also understand and assume that there will be a hit to overall performance by using them.
- VPNs will nearly always slow down traffic because they have to encrypt it over the wire, then decrypt it on the receiving end. This must be done for all packets, so it's not unusual to see your potential throughput dropped to 25% of its capacity. For example, if you have a 100Mbps down connection per workstation (typical for most home networks but most likely less in a business setting), you may find the throughput drop to 25Mbps when the VPN is connected. This is largely unavoidable due to the encryption/decryption required.
- It is possible to arrange for a private, dedicated VPN link to your Oracle Service Cloud instance. Advantages to this include an additional layer of security. You can arrange this through your Sales Manager if interested.



# Considerations over the Internet – SEC\_(IN)VALID keys

- At this point you may be wondering, without proxies or VPNs, how do I protect my site's data? The case may also be that it is impossible for you to bypass either of these, due to your local security policy.
- The best way to control access to your site is to use our suite of config verbs that begin with SEC, or SEC\_(IN)VALID (answer ID 245 in our knowledgebase). These keys give you granular control over any and all IPs/subnets or domains that are able to access the specified interface, and they are configured on a per-interface basis.
- This would allow you to theoretically block out the entire interface from the Internet with the exception of one user or one location, if so desired. This can be done for the admin console as well as the end-user pages. ***Needless to say, configured improperly this could also lead to access issues!***

# Considerations over the Internet – Domains

- Oracle Service Cloud has the following domain requirements, which should be allowed in an unrestricted manner through all your network appliances:
- \*.csthhelp.com
- \*.rightnowtech.com
- \*.rightnow.com
- \*.rntraining.com
- \*.livelook.com and \*.livelook.net (for co-browse functionality)
- \*.birst.com (for Enterprise Analytics functionality)
- \*.hivelive.com (for Oracle Social functionality)
- \*.rnengage.com
- \*.estara.com (For Engagement Engine)

# Considerations over the Internet – Domains, cont'd

- A relatively common issue we hear in support is that -- due to your security policy -- you are unable to whitelist using the full wildcard and domain, and instead must use IP addresses.
- Using IP addresses as the sole source of whitelisting creates an opening for issues when connecting to a cloud environment, as the application may make calls to multiple hosts within a certain domain for load balancing purposes, or to maintain high availability. If a problem were to ever develop, this creates a single point of failure.
- If you've exhausted all other options and absolutely must have the IP addresses, you can submit a service request and we will provide them. We provide the entire data center IP range and subnet where your instance is hosted in this scenario. We advise against going this route when it can be avoided.

# Considerations over the Internet – miscellaneous access control mechanisms

- Most organizations also employ some form of device endpoint security, tools such as McAfee Web Gateway, Norton Internet Security, Sophos, Carbon Black, you name it. There are many out there, and they all operate on similar principles for the most part.
- OSvC is a chatty and frequently evolving service, both of which can be flagged as problematic for security software. This is further compounded by the fact that you can write custom integrations to the API, or that the application's hash will change during upgrades and service packs.
- For the above reasons, we normally recommend that you whitelist the .NET application at the workstation level by using the process name in Windows, which does not change. This process is RightNow.CX.exe, and it will be the same on all your workstations, regardless of OS version or other variables.

# Considerations over the Internet – miscellaneous access control mechanisms

- Most organizations also employ some form of device endpoint security, tools such as McAfee Web Gateway, Norton Internet Security, Sophos, Carbon Black, you name it. There are many out there, and they all operate on similar principles for the most part.
- OSvC is a chatty and frequently evolving service, both of which can be flagged as problematic for security software. This is further compounded by the fact that you can write custom integrations to the API, or that the application's hash will change during upgrades and service packs.
- For the above reasons, we normally recommend that you whitelist the .NET application at the workstation level by using the process name in Windows, which does not change. This process is RightNow.CX.exe, and it will be the same on all your workstations, regardless of OS version or other variables.

# Client types – BUI vs .NET

- Long time OSvC clients will note that for many years our application was built exclusively on .NET, with dependencies on multiple services from Microsoft such as IE, ClickOnce, Windows, etc., and that within the past few years we've also implemented a browser-based version, known as BUI, or Browser User Interface. This was largely an effort to accommodate additional operating systems besides just Windows, so that Linux and Mac machines could have access to the application as well.
- Unlike the .NET application, BUI is dependent not on Windows and Microsoft technologies, but specific browser versions. By default we support major browsers like Chrome, Firefox, and Edge for BUI.
- From a networking perspective, BUI is indistinguishable from the .NET application, in that the same Oracle domains, hostnames, and IPs are used in the communication. The SEC\_(IN)VALID keys apply here as well, as they are specific to the primary vhost of the interface and are not concerned with the client type.

# Bandwidth Requirements

- The payload size of network segments will vary significantly depending on the site in question, and therefore a one-size-fits-all approach is not practical in all situations. Much of this is dependent on the way queries and other reporting functions within your site are designed.
- Our testing averages have shown that payload requests can range from 1-50KB each, with maximums reaching 100KB - 2MB. Single agent utilization may average 1-10kbps in five minute intervals, but may burst well beyond this in shorter intervals.
- Your connectivity to your data center pod should provide than a 250 ms round trip time (RTT) and less than near-zero packet loss. Where possible, your IT/IS staff should work to minimize WAN / Internet latency to ensure proper application performance. This should be easily attainable with proper configuration and a consistent route.

# Chat

- Chat utilizes a separate server that is associated to your main database server, but still unique from a networking perspective
- The chat server hostname will begin with 'bcvip', then the data center pod, and the specific server ID in the naming convention. For example, bcvipva01, bcvippc02, etc. They are all on the \*.rightnowtech.com domain just like all of our other servers.
- Diagnostics and testing for chat related issues that are suspected to be within connectivity should always use the aforementioned server, rather than your primary vhost.
- Chat may very well have the strictest networking requirements. Network connections must be steady and dependable, with minimal latency. Many times there are more domains involved in the dialogue, such as \*.estara.com, \*.livelook.com (for Co-browse) and rnengage.com. All of these work together and must be allowed through your network in an unrestricted way to avoid any issues.



# Custom Domains

- Oracle Service Cloud allows for the use of custom domains, sometimes referred to as ‘vanity URLs’. These allow you to associate your own organization’s domain to your interface, and can be protected using SSL by providing your own custom domain SSL/TLS server certificate for us to host.
- Some advantages to using a custom domain are that you do not need to share the default \*.custhelp.com space, and that you have granular control over the certificate you use on your site.
- You can use any certificate type of your choosing, such as single-domain, SAN (subject alternative name) and wildcards. Each has its own advantages and specific needs are going to be situational to the organization. SAN certificates are probably the most common, as they usually allow you to cover anywhere from 24-40 names on a single cert, depending on the cert authority.

# Custom Domains – cont'd

- Certs are applied on a per-interface basis. In general it is in your best interest to cover as many names as possible on as few certs as possible. This simplifies cert management and gives you the greatest value.
- Although it is technically possible, it is never advised to implement a custom domain unless you can also cover it with a certificate for SSL. A custom domain with no SSL certificate would use the protocol HTTP, which is sent in clear-text and offers no security for encryption, particularly risky when using the admin console, which is more likely to send sensitive data than the end-user pages. This has become increasingly important recently, as major browsers are phasing out all communications over HTTP in the coming months and years, so that sites with no valid cert would display an unsightly warning message to the end-user when they try to access.

# Connectivity troubleshooting

- In OSvC Technical Support, we often use certain tools that are useful in many different types of situation. For troubleshooting network issues, we prefer to use a combination of Fiddler, Wireshark, and Traceroute.
- Fiddler acts like a proxy (in fact you can even see it replace the workstation's default proxy while it's running). This allows it to sit between the client device and server and capture all communications over HTTP/HTTPS between the two, which is very helpful for finding the cause of issues that are not necessarily apparent on the surface. What we like to look for in Fiddler results are the timings of network transactions, the hosts involved, and the response codes from the server.

# Connectivity troubleshooting – cont'd

- Wireshark is commonly used by networking and security professionals alike, as it gives a microscopic view of *all* data visible to the network interface that is queried. For this reason we typically like to use it when issues are not fully revealed in Fiddler, or when there is other traffic on the network that may be interfering. It is best used in combination with Fiddler so that we can match the corresponding timestamps, and get the best possible picture.
- Traceroute is another commonly used diagnostic utility. We have a tool called the Persistent Traceroute, which is a low-resource batch file that runs in the background while the agent is working, and logs the traceroute output into a text file. It is ideal to allow this tool to run for about 30 minutes if possible, so that we can see the most accurate reflection of the network state. This tool is most effective when the issue is suspected to be within the route from the client device to the data center.

# Connectivity troubleshooting – additional considerations

- The best case scenario for us to be able to see the issue in full detail, is to try to run as many tools as you can simultaneously, within reason. Doing so minimizes the amount of time required for us to investigate, and minimizes the need to request additional information down the road. If you can run these captures while also running a video of the issue, that is even better, as it allows us to follow along exactly.
- Whenever practical, it is best to also provide us steps to reproduce. Some issues may appear to be network related when in fact they are more likely to be somewhere within the database tier, or within the affected user profile. Having detailed steps to reproduce, including affected agent accounts, helps us to provide a quick resolution, and determine if the issue is truly within the network, or perhaps elsewhere in the product
- Many organizations block ICMP, which is the protocol used by ping and traceroute. This is done mainly because of their potential for misuse. You may find that running a traceroute on the machine is not returning the expected results, in which case you should reach out to the local IT admin/security team to assist if necessary.

# Question and Answer Segment

- At this point we will open up the discussion to anyone interested in asking questions on the topics covered, or anything else you believe pertinent to the concept of networking and OSvC.



# Oracle Service Cloud Support Webinars

- Service Request
- Support Hotline
- Updates
- Suggestion Box
- Manager Connect

Submit a Service Request

## Upcoming Webinars

### Demystifying CPMs **New**

**Scheduled:** Wed June 06th, 2018 9:00 am MDT

**Presenter:** Johnny Meehan

**Description:**

Walk through the development of a CPM (Custom Process Model), including the idiosyncrasies of implementing a test harness. Learn how to effectively debug during development as well as live usage.

Register

### Managing and Monitoring OSvC Health **New**

**Scheduled:** Wed July 11th, 2018 2:09 pm MDT

**Presenter:** Owen Sood-Giddings

**Description:**

There's a lot going on in your support organization and a lot going on in your site. Let Owen talk you through some ways Oracle's own instance of OSvC is implemented to help the Technical Support team monitor potential issues, keep the site organized, implement fixes & enhancements, and keep versions and frameworks up to date.

Register

Have a suggestion for a webinar topic? [Send us your idea!](#)