修改访问配置须知

修改访问配置前，用户需根据不同场景进行准备条件检查。以下是三个修改配置场景及所需的准备条件、操作步骤：

场景一：使用外部反向代理发布 AnyShare 应用，设置访问地址为外网 IP（如为公有云部署，则反向代理位置修改为公有云负载均衡器）

- **预备条件：**
  1、 在 AnyShare 部署控制台访问【站点配置】-【访问配置】页面，将反向代理 IP 添加至 **访问规则**；
  2、 反向代理需反代所有内外部所需端口，包括更新后的文档域和对象存储访问端口；
  3、 检查确认 AnyShare 集群内服务均正常；
  4、 检查确认更新后的端口在 AnyShare 集群内所有节点均未占用；
  5、 检查确认反代服务器与 AnyShare 集群时间一致；

请确保以上条件均已满足，再按照下方步骤进行修改访问配置操作。

C

- **操作步骤：**
  1、 在 AnyShare 部署控制台访问【站点配置】-【访问配置】页面，将访问地址修改为外部反向代理 IP，修改端口为所需端口；
  2、 修改失败时，需要按照提示信息纠正错误，再继续修改；
  3、 修改成功后，将自动跳转至新的访问地址，此时由于证书不匹配，在部署控制台页面和 OAuth2.0 认证页面均会出现证书警告，需手动按照浏览器提示忽略证书警告；
  4、 重新登录进入 AnyShare 部署控制台后，访问【站点配置】—【HTTPS 证书配置】页面，按需上传 CA 机构证书，或者一键生成自签名证书；
  5、 通过访问 AnyShare Web 客户端验证确认配置成功；

场景二：使用外部反向代理发布 AnyShare 应用，设置访问地址为指向外部反向代理 IP 的域名（如为公有云部署，则反向代理位置修改为公有云负载均衡器）

- **预备条件：**
  1、 在 AnyShare 部署控制台访问【站点配置】-【访问配置】页面，将反向代理 IP 添加至 AnyShare 防火墙规则；
  2、 在 AnyShare 部署控制台访问【站点配置】-【DNS 配置】页面，按照实际情况设置可用的 DNS 服务器；
  3、 反向代理需反代所有内外部所需端口，包括更新后的文档域和对象存储访问端口；
  4、 检查确认 AnyShare 集群内服务均正常；
  5、 检查确认待配置的域名可正常解析为反向代理 IP；
  6、 检查确认更新后的端口在 AnyShare 集群内所有节点均未占用；

7、 检查确认反代服务器与 AnyShare 集群时间一致；

请确保以上条件均已满足，再按照下方步骤进行修改访问配置操作。

- **操作步骤**
  1、 在 AnyShare 部署控制台访问【站点配置】-【访问配置】页面，将访问地址修改为指向外部反向代理 IP 的域名，修改端口为所需端口；
  2、 修改失败时，需要按照提示信息纠正错误后继续修改；
  3、 修改成功后，将自动跳转至新的访问地址，此时由于证书不匹配，在部署控制台页面和 OAuth2.0 认证页面均会出现证书警告，需手动按照浏览器提示忽略证书警告；
  4、 重新登录进入 AnyShare 部署控制台后，访问【站点配置】-【HTTPS 证书配置】页面，按需上传 CA 机构证书，或者一键生成自签名证书；
  5、 通过访问 AnyShare Web 客户端验证确认配置成功；

场景三：使用 NAT 映射方式发布 AnyShare 应用，设置访问地址为域名，域名内部网络解析为 AnyShare 集群 VIP，外部网络解析为 NAT 映射对应公网 IP

- **预备条件：**
  1、 在 AnyShare 部署控制台访问【站点配置】-【DNS 配置】页面，按照实际情况设置可用的 DNS 服务器；
  2、 按需添加 NAT 映射规则；
  3、 检查确认 AnyShare 集群内服务均正常；
  4、 检查确认待配置的域名内部网络可正常解析为 AnyShare 集群 VIP，外部网络可正常解析为 NAT 映射对应公网 IP；
  5、 检查确认更新后的端口在 AnyShare 集群内所有节点均未占用；

请确保以上条件均已满足，再按照下方步骤进行修改访问配置操作。

- **操作步骤：**
  1、 在 AnyShare 部署控制台访问【站点配置】-【访问配置】页面，将访问地址修改为预先准备的域名，修改端口为所需端口；
  2、 修改失败时，需要按照提示信息纠正错误后继续修改；
  3、 修改成功后，将自动跳转至新的访问地址，此时由于证书不匹配，在部署控制台页面和 OAuth2.0 认证页面均会出现证书警告，需手动按照浏览器提示忽略证书警告；
  4、 重新登录进入 AnyShare 部署控制台后，访问【站点配置】-【HTTPS 证书配置】页面，按需上传 CA 机构证书，或者一键生成自签名证书；

注：

1、 使用自签名证书时，需要自行下载自签名证书的 CA 证书，并安装至客户机的“受信任的根证书颁发机构”处；

2、 端口列表文档：AnyShare://AnyShare 研发线/7-AnyShare 系统测试部/公共文件夹/AnyShare 7.0.0/正式版/文档/部署指导文档/公有云负载均衡开放端口.docx；
3、 如遇到修改失败集群不可用情况，请联系爱数技术人员支持。

修改存取設定須知

修改存取配置前，使用者需根據不同場景進行準備條件檢查。以下是三個修改設定場景及所需的準備條件、操作步驟：
場景一：使用外部反向代理髮布 AnyShare 應用，設定存取地址為外部反向代理 IP（如為公有云部署，則反向代理位置修改為公有云負載均衡器）

預備條件：
1、 在 AnyShare 部署主控台存取【站台設定】-【站台設定】頁面，將反向代理 IP 添加至 AnyShare 防火牆規則；
2、 反向代理需反代所有內外部所需埠口，包括更新後的文件網域和物件儲存存取埠口；
3、 檢查確認 AnyShare 集群內服務均正常；
4、 檢查確認更新後的埠口在 AnyShare 集群內所有節點均未佔用；
5、 檢查確認反代服務器與 AnyShare 集群時間一致；

請確保以上條件均已滿足，再按照下方步驟進行修改存取設定操作。

操作步驟：
1、 在 AnyShare 部署主控台存取【站台設定】-【存取設定】頁面，將存取位址修改為外部反向代理 IP，修改埠口為所需埠口；
2、 修改失敗時，需要按照提示資訊糾正錯誤，再繼續修改；
3、 修改成功後，將自動跳轉至新的存取位址，此時由於證書不匹配，在部署主控台頁面和 OAuth2.0 認證頁面均會出現證書警告，需手動按照瀏覽器提示忽略證書警告；
4、 重新登錄進入 AnyShare 部署主控台後，存取【站台設定】—【HTTPS 證書設定】頁面，按需上傳 CA 機構證書，或者一鍵生成自簽名證書；
5、 通過存取 AnyShare Web 客戶端驗證確認設定成功；

場景二：使用外部反向代理髮布 AnyShare 應用，設定存取位址為指向外部反向代理 IP 的域名（如為公有云部署，則反向代理位置修改為公有云負載均衡器）

預備條件：
1、 在 AnyShare 部署主控台存取【站台設定】-【存取設定】頁面，將反向代理 IP 添加至 AnyShare 防火牆規則；
2、 在 AnyShare 部署主控台存取【站台設定】-【DNS 設定】頁面，按照實際情況設定可用的 DNS 服務器；
3、 反向代理需反代所有內外部所需埠口，包括更新後的文件網域和物件儲存存取埠口；
4、 檢查確認 AnyShare 集群內服務均正常；
5、 檢查確認待設定的域名可正常解析為反向代理 IP；

6、 檢查確認更新後的埠口在 AnyShare 集群內所有節點均未佔用；
7、 檢查確認反代服務器與 AnyShare 集群時間一致；

請確保以上條件均已滿足，再按照下方步驟進行修改存取設定操作。

操作步驟
1、 在 AnyShare 部署主控台存取【站台設定】-【存取設定】頁面，將存取位址修改為指向外部反向代理 IP 的域名，修改埠口為所需埠口；
2、 修改失敗時，需要按照提示資訊糾正錯誤後繼續修改；
3、 修改成功後，將自動跳轉至新的存取位址，此時由於證書不匹配，在部署主控台頁面和 OAuth2.0 認證頁面均會出現證書警告，需手動按照瀏覽器提示忽略證書警告；
4、 重新登錄進入 AnyShare 部署主控台後，存取【站台設定】-【HTTPS 證書設定】頁面，按需上傳 CA 機構證書，或者一鍵生成自簽名證書；
5、 通過存取 AnyShare Web 客戶端驗證確認設定成功；
場景三：使用 NAT 映射方式發布 AnyShare 應用，設定存取位址為域名，域名內部網絡解析為 AnyShare 集群 VIP，外部網絡解析為 NAT 映射對應公網 IP

預備條件：
1、 在 AnyShare 部署主控台存取【站台設定】-【DNS 設定】頁面，按照實際情況設定可用的 DNS 服務器；
2、 按需添加 NAT 映射規則；
3、 檢查確認 AnyShare 集群內服務均正常；
4、 檢查確認待設定的域名內部網絡可正常解析為 AnyShare 集群 VIP，外部網絡可正常解析為 NAT 映射對應公網 IP；
5、 檢查確認更新後的埠口在 AnyShare 集群內所有節點均未佔用；

請確保以上條件均已滿足，再按照下方步驟進行修改存取設定操作。

操作步驟：
1、 在 AnyShare 部署主控台存取【站台設定】-【存取設定】頁面，將存取位址修改為預先準備的域名，修改埠口為所需埠口；
2、 修改失敗時，需要按照提示資訊糾正錯誤後繼續修改；
3、 修改成功後，將自動跳轉至新的存取位址，此時由於證書不匹配，在部署主控台頁面和 OAuth2.0 認證頁面均會出現證書警告，需手動按照瀏覽器提示忽略證書警告；
4、 重新登錄進入 AnyShare 部署主控台後，存取【站台設定】-【HTTPS 證書設定】頁面，按需上傳 CA 機構證書，或者一鍵生成自簽名證書；

注：
1、 使用自簽名證書時，需要自行下載自簽名證書的 CA 證書，並安裝至客戶機的“受信任的根證書頒發機構”處；
2、 埠口列表文件：AnyShare://AnyShare 研發線/7-AnyShare 系統測試部/公共文件夾/AnyShare 7.0.0/正式版/文件/部署指導文件/公有云負載均衡開放埠口.docx；
3、 如遇到修改失敗集群不可用情況，請聯繫愛數技術人員支持。

Notes for Changing Access Configuration

You are required to check your prerequisite settings before changing your Access Configuration. Below are the three scenarios and the corresponding settings as well as its procedures.

Scenario 1

AnyShare is released with external reverse proxy and the access address is set as external network IP. (If it is deployed in Public Cloud, then the reverse proxy address should be changed to load balancer for public cloud.)

Prerequisites

1. In **Site Configuration→Access Configuration**, add the reverse proxy to **Access Rule**.
2. Set all the necessary ports as reverse proxy including those updated in document domains and object storage.
3. Make sure that all the services are normal in AnyShare clusters.
4. Ensure that all the ports in AnyShare cluster nodes are not occupied.
5. Ensure the time of reverse proxy is the same as that of AnyShare Clusters

If all the conditions above are met, then you can change Configuration in the following steps.

Steps

1. In **Site Configuration→Access Configuration**, change the access address as the IP of external reverse proxy IP, and change the ports as needed.
2. If it fails, you need to fix the error based on the tips and change them again.
3. After it is modified successfully, the page will jump to the new address. Since the license is not matched, a warning notice will appear in Deployment Console page and the OAuth 2.0 page. You need to skip the notice in your browser.
4. Enter AnyShare Deployment Console and go to **Site Configuration→HTTPS Certificate** page, where you can upload the CA certificate or generate the Self-signed certificate.
5. Verify your settings in AnyShare for Web

Scenario 2

AnyShare is released with external reverse proxy and the access address is set as the orientation of external reverse proxy domain name. (If it is deployed in Public Cloud, then the reverse proxy address should be changed to load balancer for public cloud.)

Prerequisites

1. In **Site Configuration→Access Configuration**, add the reverse proxy to **Access Rule**.
2. Set the DNS server in **Site Configuration→DNS Configuration**.
3. Set all the necessary ports as reverse proxy including those updated in document domains and object storage.
4. Make sure that all the services are normal in AnyShare clusters.
5. Make sure that all the domain names to be set can be parsed to reverse proxy IP.
6. Ensure that all the ports in AnyShare cluster nodes are not occupied.
7. Ensure the time of reverse proxy server is the same as that of AnyShare Cluster.

If all the conditions above are met, then you can change Configuration in the following steps.

Steps

1. In **Site Configuration→Access Configuration**, change the access address to the domain name which points to the external reverse proxy IP, and change the ports as needed.
2. If it fails, you need to fix the error based on the tips and change them again.
3. After it is modified successfully, the page will skip to the new address. Since the license is not matched, a warning notice will appear in Deployment Console page and the OAuth 2.0 page. You need to skip the notice in your browser.
4. Enter AnyShare Deployment Console and go to **Site Configuration→HTTPS Certificate** page, where you can upload the CA certificate or generate the Self-certificate
5. Verify your settings in AnyShare for Web

Scenario 3

AnyShare is released in NAT mapping mode, andthe access address is set as the domain name.

Inside the domain name, the internal network is parsed as AnyShare Cluster VIP, while outside, the external network is parsed as NAT mapping, corresponding with the public network IP.

Prerequisites

1. Set the DNS server in **Site Configuration→DNS Configuration**.
2. Add the NAT mapping rules as required.
3. Make sure that all the services are normal in AnyShare clusters.
4. Ensure that inside the domain name, the internal network is parsed as AnyShare Cluster VIP, while outside, the external network is parsed as NAT mapping, corresponding with the public network IP.
5. Ensure that all the ports in AnyShare cluster nodes are not occupied.

If all the conditions above are met, then you can change Configuration in the following steps.

Steps

1. In **Site Configuration→Access Configuration**, change the access address as the IP of external reverse proxy IP, and change the ports as needed.
2. If it fails, you need to fix the error based on the tips and change them again.
3. After it is modified successfully, the page will skip to the new address. Since the license is not matched, a warning notice will appear in Deployment Console page and the OAuth 2.0 page. You need to skip the notice in your browser.
4. Enter AnyShare Deployment Console and go to **Site Configuration→HTTPS Certificate** page, where you can upload the CA certificate or generate the Self-signed certificate

Note:

1. For Self-signed certificate, you will need to download the self-signed certificate and install it to Trusted root Certification Authorities.
2. Documents for port list: AnyShare://AnyShare 研发线/7-AnyShare 系统测试部/公共文件夹/AnyShare 7.0.0/正式版/文档/部署指导文档/公有云负载均衡开放端口.docx
3. If you find clusters unavailable, feel free to contact our technicians for help.