



VMware UAG As Built Report

YOUNGTECH

Author: Chris Hildebrandt
Date: Friday, February 2, 2024
Version: 1.0.0

Table of Contents

1 Universal Access Gateway (UAG) - UAG2	3
1.1 General Settings	3
1.1.1 Edge Service Settings.....	3
1.1.1.1 Horizon Settings - UAG2	3
1.1.2 Authentication Settings	4
1.2 Advanced Settings	4
1.2.1 Advanced Settings	4
1.2.1.1 System Configuration	4
1.2.1.2 Network Settings	6
1.2.1.3 High Availability Settings	6
1.2.1.4 TLS Server Certificate Settings	6
1.2.1.4.1 User TLS Server Certificate Settings.....	6
1.2.1.4.2 Admin TLS Server Certificate Settings	7
1.2.1.5 Account Settings.....	7
1.2.1.5.1 Account Settings - admin.....	7
1.2.2 Identity Bridging Settings	8
1.3 Support Settings	8
1.3.1 Support Settings.....	8
1.3.1.1 Log Level Settings.....	8

1 Universal Access Gateway (UAG) - UAG2

The following section provides a summary of the implemented components on the VMware UAG infrastructure.

1.1 General Settings

1.1.1 Edge Service Settings

The following section will provide details on Edge Service Settings on the UAG - UAG2.

1.1.1.1 Horizon Settings - UAG2

Enable Horizon	Yes
Connection Server URL	https://HRZ.chrislab.com:443
Minimum SHA Hash Size	Default
Connection Server URL Thumbprint	sha256=2E:7E:7B:15:D2:12:9D:49:D2:11:28:CD:8F:3E:4F:C3:86:A3:7C:0E:4B:DC:AB:AF:71:91:32:02:1C:F5:01:EB
Honor Connection Server Redirect	No
Connection Server IP Mode	IPV4
Client Encryption Mode	ALLOWED
Auth Methods	--
Identity Provider	--
SAML Audiences	--
SAML Unauthenticated Username Attribute	--
Default Unauthenticated Username	--
Health Check URI Path	/favicon.ico
Re-Write Origin Header	No
Enable PCOIP	No
Disable PCOIP Legacy Certificate	No
PCOIP External URL	IPV4
Enable Blast	Yes
Blast External URL	https://HRZ.chrislab.com:8443
Enable UDP Tunnel Server	Yes
Blast Proxy Certificate	--
Blast Allowed Host Header Values	--
Enable Tunnel	Yes
Tunnel External URL	https://HRZ.chrislab.com:443
Tunnel Proxy Certificate	--
Endpoint Compliance Check Provider	--
Proxy Pattern	(/ /view-client(.*) /portal(.*) /appblast(.*))
Enable Proxy Pattern Canonical Match	Yes
SAM SP	--
User Name Label for RADIUS	--
Passcode Label for RADIUS	--
Logout On Certificate Removal	No
Match Windows User Name	Yes

Gateway Location	External
Enable Windows SSO	Yes
RADIUS Class Attributes	--
Disclaimer Text	--
Show Connection Server Pre-Login Message	Yes
Trusted Certificates	--
Response Security Headers	Strict-Transport-Security : max-age=63072000; includeSubdomains; preload X-XSS-Protection : 1; mode=block X-Content-Type-Options : nosniff Content-Security-Policy : default-src 'self';font-src 'self' data:;script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style- src 'self' 'unsafe-inline';img-src 'self' blob: data: X-Frame-Options : SAMEORIGIN
Client Custom Executables	--
Host Port Redirect Mappings	--
Host Entries	--
Disable HTML Access	No

Table 1 - Horizon Settings Summary - UAG2

1.1.2 Authentication Settings

1.2 Advanced Settings

1.2.1 Advanced Settings

1.2.1.1 System Configuration

The following section will provide details on System Configuration Settings on the UAG - UAG2.

UAG Name	UAG2.chrislab.local
Password Age	90
Monitoring User Password Age	90
Root Password Age	0
Admin Password Policy Settings	@{passwordPolicyMinLen=8; passwordPolicyMinClass=1; passwordPolicyDifok=4; passwordPolicyUnlockTime=5; passwordPolicyFailedLockout=3}
Password Policy Settings	@{passwordPolicyMinLen=6; passwordPolicyMinClass=1; passwordPolicyDifok=4; passwordPolicyUnlockTime=900; passwordPolicyFailedLockout=3}
IP Mode	STATICV4
FIPs Mode	No

VMware UAG As Built Report - v1.0.0

DS Compliance OS	No
OS Login Username	administrator@vsphere.local
Admin Cert Rollback Enabled	No
TLS Server Cipher Suites	TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_CHACHA20_POLY1305_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS Client Cipher Suites	--
Enable TLS 1.0	No
Enable TLS 1.1	No
Enable TLS 1.2	Yes
Enable TLS 1.3	Yes
Enable SSLv3	No
SSL Provider	OPENSSL
TLS Named Groups	--
TLS Signature Schemes	--
TLS Port Sharing	Yes
Allowed Host Headers	--
Health Check URL	/favicon.ico
HTTP Health Monitor	No
Unrecognized Sessions Monitoring Enabled	Yes
Cookies to be Cached	none
Quiesce Mode	No
Monitor Interval	60
Enable SAML Certificate Rollover Support	No
Authentication Timeout	300000
Body Receive Timeout	15000
Maximum Connections per Session	16
Client Connection Idle Timeout	360
Request Timeout	10000
Http Connection Timeout	120
Admin Max Concurrent Sessions	5
Admin Session Idle Timeout	10
Root Session Idle Timeout	300
OS Max Login Limit	10
Clock Skew Tolerance	600
Max Allowed System CPU Usage	100
Session Timeout	36000000
Join CEIP	Yes
Enable SNMP	No
SNMP Settings	version ----- V1_V2C

Admin Disclaimer Text	--
DNS	172.16.50.10 172.16.50.11
DNS Search	chrislab.local
Time Sync with Host	--
Host Clock Sync Enabled	No
Host Clock Sync Supported	Yes
NTP Servers	--
Fallback NTP Servers	--
Extended Server Certificate Validation	No
SSH Enabled	No
SSH Password Access Enabled	Yes
SSH Key Access Enabled	No

Table 2 - System Configuration - UAG2

The following section will provide details for Network Settings on the UAG - UAG2.

1.2.1.2 Network Settings

NIC	eth0
IPv4 Address	172.16.50.33
IPv4 Subnet	255.255.255.0
IPv4 Gateway	172.16.50.1
IP Allocation Mode	STATICV4
Static Routes	--
Custom Configuration	--

Table 3 - Network Settings - UAG2

The following section will provide details for High Availability Settings on the UAG - UAG2.

1.2.1.3 High Availability Settings

High Availability Mode	ONEARM
High Availability State	--
Virtual IP Address	172.16.40.99
Group ID	42

Table 4 - High Availability Settings - UAG2

1.2.1.4 TLS Server Certificate Settings

The following section will provide details for Admin TLS Server Certificate Settings on the UAG - UAG2.

1.2.1.4.1 User TLS Server Certificate Settings

Admin TLS Server Cert Configured	Yes
Common Name	*.chrislab.local
Organization	Chrislab
Issuer Name	CN=ChrisLab-DC2-CA, DC=ChrisLab, DC=local
Valid From	09/27/2023 16:14:25
Valid To	09/26/2024 16:14:25
Friendly Name	--
Serial Number	1400000F2954481CCF49018F65000000000F29
Thumbprint	F61671A8765A91EF7F8BCEF9535C5A4DE0A42801
Includes Private Key	No
DNS List	*.chrislab.local
Subject Name	CN=*.chrislab.local, OU=IT, O=Chrislab, L=Ottawa, S=KS, C=US
Version	3
Handle	1990416968672

Table 5 - User Server Certificate Settings - UAG2

1.2.1.4.2 Admin TLS Server Certificate Settings

Admin TLS Server Cert Configured	Yes
Common Name	*.chrislab.local
Organization	Chrislab
Issuer Name	CN=ChrisLab-DC2-CA, DC=ChrisLab, DC=local
Valid From	09/27/2023 16:14:25
Valid To	09/26/2024 16:14:25
Friendly Name	--
Serial Number	1400000F2954481CCF49018F65000000000F29
Thumbprint	F61671A8765A91EF7F8BCEF9535C5A4DE0A42801
Includes Private Key	No
DNS List	*.chrislab.local
Subject Name	CN=*.chrislab.local, OU=IT, O=Chrislab, L=Ottawa, S=KS, C=US
Version	3
Handle	1990416960736

Table 6 - Admin Server Certificate Settings - UAG2

1.2.1.5 Account Settings

The following section will provide details on Account Settings on the UAG - UAG2.

1.2.1.5.1 Account Settings - admin

Name	admin
User ID	a3c8be9d-4d4c-43ae-b471-5e8f24728e5a
Enabled	Yes

Roles	ROLE_ADMIN
Password Last Set	2024-01-23T16:26:51.854539Z[Etc/UTC]
Days till Password Expires	80
User Type	INTERNAL

Table 7 - Account Settings - admin

1.2.2 Identity Bridging Settings

1.3 Support Settings

1.3.1 Support Settings

The following section will provide details for Log Level Settings on the UAG - UAG2.

1.3.1.1 Log Level Settings

All	info
Admin	--
Horizon Edge Service - All	--
Horizon Edge Service - XMLAPI	--
Horizon Edge Service - Authentication	--
Horizon Edge Service - Blast	--
Horizon Edge Service - Tunnel	--
Horizon Edge Service - PCOIP	--
Horizon Edge Service - UDP Tunnel	--
Server	--
Horizon Edge Service - Endpoint Compliance	--
Web Reverse Proxy Edge Service - All	--

Table 8 - Radius Settings - UAG2