

Proof of Concept Prerequisites Checklist

Customer: _____

Products:

- Cygn Auditor for Active Directory
- Cygn Auditor for AWS
- Cygn Auditor for File System
- Cygn Auditor for Azure
- Cygn Auditor for Microsoft 365
- Cygn Auditor for On-Premises Exchange
- Cygn Auditor for VMware
- Cygn Auditing & Security Suite (PBMS)


Before conducting a PoC, customers are advised to check the following prerequisites and prepare the test environment accordingly.

| DEPARTMENT | SOURCE | REQUIREMENTS | DUE DATE | STATUS |
|---------------------|--------|--|----------|--------|
| Server | All | <p>Two available virtual machines:</p> <ol style="list-style-type: none"> 1. Application server: A clear Windows Server 2019 with preinstalled IIS (including Windows Authentication, ASP.NET) and .Net Framework 4.8. Featuring any modern processor, 4 GB RAM (min) or 8 GB RAM (recommended), HDD 100 MB. 2. Database server: Any server with SQL Server 2019 Standard Edition. Featuring minimum 2 GB free storage space, 8 GB RAM (min) or 16 GB RAM (recommended). | | |
| Firewall / Security | All | <p>Firewall should allow the following inbound and outbound connections:</p> <ul style="list-style-type: none"> • Application server: 80 or 443 TCP port for inbound connections; 135, 443, and 1433 TCP ports for outbound connections. And specifically allow HTTPS access to the following Microsoft 365 and AWS URLs: <ul style="list-style-type: none"> cygnacloud.azurewebsites.net (GET and POST) graph.microsoft.com (GET only) login.microsoftonline.com (GET only) login.windows.net (GET only) *.microsoftonline-p.com (GET only) manage.office.com (GET only) management.azure.com (GET only) *.amazonaws.com (GET and POST) | | |

| DEPARTMENT | SOURCE | REQUIREMENTS | DUE DATE | STATUS |
|---------------------|--------------------------------------|---|----------|--------|
| | | <ul style="list-style-type: none"> • To see online help, you will also need access to: docs.cygnalabs.com. For agent-based Active Directory auditing, allow access to: msdl.microsoft.com/download/symbols msdl.microsoft.com *.core.windows.net (GET) • Database server: 1433 TCP port for inbound connections. • Domain controllers and file servers: 1433 TCP port for outbound connections, 445 and 139 TCP ports for inbound connections. | | |
| Firewall / Security | Azure AD Microsoft 365 AWS | <ul style="list-style-type: none"> • If your company restricts access to network resources, set up a proxy server to reroute Cygna Auditor traffic. • Verify that your proxy server allows connections to the following Microsoft 365 and AWS URLs: cygnacloud.azurewebsites.net (GET and POST) graph.microsoft.com (GET only) login.microsoftonline.com (GET only) login.windows.net (GET only) *.microsoftonline-p.com (GET only) manage.office.com (GET only) | | |

| DEPARTMENT | SOURCE | REQUIREMENTS | DUE DATE | STATUS |
|-----------------|------------------|--|----------|--------|
| | | <p>management.azure.com (GET only)</p> <p>*.amazonaws.com (GET and POST)</p> | | |
| Domain | All | Configured and fully functioning Active Directory domain. | | |
| Domain / Server | All | <p>The following accounts in hand for the product installation and PoC:</p> <ul style="list-style-type: none"> • Domain administrator account. This account should be authorized to perform test activity in your PoC environment. • Account with access to VMware logs. • SQL Server account with the dbcreator server role. | | |
| Domain | Active Directory | <p>Auditing configuration:</p> <ul style="list-style-type: none"> • Group Policy Management is enabled on Cygna Auditor host. The group policies Audit account management, Audit directory service access, Audit object access, Audit User Account Management, Audit Computer Account Management, Audit directory service changes, Audit Distribution Group Management, Audit Security Group Management, and Audit Account Lockout should be set to <i>"Success"</i> and <i>"Failure"</i>. The policies Account lockout duration and Reset account lockout counter after should be set to <i>"30 minutes"</i> and Account lockout threshold to <i>"5 invalid logon attempts"</i>. | | |

| DEPARTMENT | SOURCE | REQUIREMENTS | DUE DATE | STATUS |
|------------|---|---|----------|--------|
| | | <p>The policy Audit Kerberos Authentication Service should be set to <i>"Failure"</i>.</p> <ul style="list-style-type: none"> Allowed remote access to DC's event logs with Remote event log management (RPC-EPMAP) and Remote event log management (RPC) firewall rules. ACLs configured for Default naming context and Configuration naming context. (only for AD Recovery) Changes to Schema naming context including updates to the searchFlags attributes of password-related objects and SID History objects. | | |
| Server | File System | <p>Auditing configuration:</p> <ul style="list-style-type: none"> Enabled firewall rules: Netlogon Service (NP-In), File and Printer Sharing (SMB-In), File Server Remote Management (SMB-In). | | |
| Mail | Exchange Online On-Premises Exchange | <p>Auditing configuration:</p> <ul style="list-style-type: none"> Enabled mailbox logging and configure auditing of all actions for all user mailboxes in your Exchange Online or on-premises Exchange organization. | | |
| Cloud | Recovery for Azure AD | <p>Register the Cygna Auditor app in your Azure AD and grant it API permissions to collect snapshots of Azure AD. Generate a key and secret to query this data.</p> | | |

 **Note:** For more information about Cygna Auditing & Security Suite (former PowerBroker Management Suite), including system requirements, installation procedures, and configuration steps, please refer to CA&SS documentation online.