

Centrify Zero Trust Privilege Services Standard Jump Start – 300

The Centrify Zero Trust Privilege Services Standard Jump Start 300 package is intended for environments with 300 or fewer Unix/Linux or Windows systems that make up the corporate enterprise. It is designed to give these enterprises the hands-on training and experience required to get a quick start on the deployment by implementing our Zero Trust Privilege best practices and utilizing our experienced consultants. The service eleven (11) days of consulting assistance deploying a pilot environment (up to 25 systems) and a design document detailing the customer's current environment and specific Centrify architecture, design, and processes implemented to assist in completing the overall deployment.

Benefits

- Achieve up to 50% faster time-to-production
- Gain hands-on experience deploying the Centrify Zero Trust Privilege solution
- Gain hands-on experience configuring critical processes before implementing in a production environment
- Reduced management overhead
- A consistent, supportable implementation based on your existing business practices
- Reduced troubleshooting complexity
- A scalable Centrify Zero Trust Privilege maturity model to strengthen your security posture

Enabled Capabilities

The following Zero Trust Privilege services will be deployed:

- Credential Management: account password vault, secrets vault, SSH key management; centralized management of service, shared, application accounts
- Bastion Host, Secured Remote Access via RDP and SSH
- Multi-factor Authentication for vault access, login and privilege elevation
- Authentication Services: AD bridging, local account & group management, identity consolidation
- Privilege elevation with least privilege and just-in-time access
- Desktop Apps privilege for Windows
- Gateway session monitoring and control

Deliverables

At the completion of the service, you will receive the following:

- Centrify Design Document
- Centrify Zero Trust Privilege Services, Standard Edition software deployed on up to 25 systems.

- Up to five (5) Roles for privilege elevation.
- Centrify Reporting Services (CRS) installed and report templates shared so your team can build your own custom report queries.

Duration

- Four (4) days of instructor lead Standard Training before the project begins.
- Eleven (11) days of remote consulting service. (If on-site consulting is preferred, travel expenses will be invoiced back to customer at actual cost).

Who Should Attend

Unix/Linux, Windows, Security and/or System Administrators who need to deploy and administer Centrify Zero Trust Privilege Services in their environment.

Prerequisites

- The participants should have a basic understanding of Windows, Active Directory and UNIX/Linux user authentication.
- Intended for IT environments with no more than 300 Windows, UNIX or Linux systems for the enterprise.
- Identify up to 25 systems in the environment to deploy Centrify services.
- Centrify adcheck utility run across targeted Unix/Linux systems
- Targeted Windows systems joined to Active Directory domain.
- All issues reported by the Centrify adcheck utility resolved prior to engaging with a Professional Services consultant.
- Approval to create an Organizational Unit for storage of Centrify data in targeted AD domain prior to engaging with a Professional Services consultant.
- Individual with appropriate Active Directory permissions is available during Professional Services engagement.
- All Change Control required for implementation of Centrify Zero Trust Privilege Services, Standard Edition must be approved prior to the Professional Services engagement.
- Identify all legacy NIS, LDAP or Kerberos realms that will require identity consolidation.

- Service does not include integration with LDAP proxy, SAMBA or network storage devices.
- **Note: All UNIX groups and systems, Provisioning Groups, Service Accounts, Role Groups, Licenses, Zone Administration Groups and Zones must be stored under a single organizational unit in accordance with Centrifly best practices.**

System Requirements for Training

For each student, the customer needs to provide a computer that meets or exceeds the minimum hardware requirements listed below:

- 4GB Memory
- 64-bit Operating System
- Dual-core processor
- A stable internet connection
- An HTML5 browser
- The latest version of Java

Each student machine must be verified using this URL: <https://use.cloudshare.com/Ent/Machine.mvc/testpage>

Daily Overview

DAY	DESCRIPTION
1- 4	<p>Centrifly Professional Services conducts our 4-day training for Centrifly Zero Trust Privilege Services, Standard Edition including topics covering:</p> <ul style="list-style-type: none"> • Installation, Setup and Configuration of Centrifly Zero Trust Privilege Services • Troubleshooting and remediation of deployment issues • Planning and creating Zones • Importing users and Groups into Zones • Roles Groups, Role Overrides and Provisioning Groups • Adding new user and group profiles • Mapping and migrating UNIX Service accounts in Active Directory • Removing legacy data
5	<p>Centrifly Professional Services begins our 7-day design process with activities covering the following areas:</p> <ul style="list-style-type: none"> • Completion of Design questionnaire and review of project objects • Design review and Active Directory storage structure decisions • Compare in-scope UNIX users to Active Directory users • Zone design discussion to determine Parent and Child Zone configuration • Roles, Rights discussion for personnel and Computer Roles • Planning for Centrifly Zero Trust Privilege Services, Standard Edition deployment and on-going configuration management of UNIX Group policies • Review of final design document draft with cross functional team
6 - 10	<p>Centrifly Professional Services begins Centrifly Suite Standard Edition deployment and continues with design activities including:</p> <ul style="list-style-type: none"> • Centrifly Zero Trust Privilege Services, Standard Edition is installed (via Deployment Manager) on all in-scope deployment targets. Note: Centrifly Zero Trust Privilege Services, Standard Edition is not started, and users and groups are not migrated. • One-week soak period begins • Design activities continue for the customer environment

Pricing and Ordering

This offering is invoiced on purchase and is valid for 6 months from the date of purchase. Contact your Centrifly Sales representative for pricing details for your region and to arrange for a time, place, and schedule. Or email us at sales@centrifly.com.

Customizations

The Centrifly Professional Services team has the skill and expertise to handle or assist with many implementation customizations where needed. If there are extra implementation tasks that are required, custom scripting needs, custom integration requirements, or any other technical services that will be useful to customer success with Centrifly, our services team can set up a pre-sale scoping call to provide custom implementation estimates to fulfill these needs.

DAY	DESCRIPTION
11	<p>Active Directory Setup</p> <p>Key topics:</p> <ul style="list-style-type: none"> • All Active Directory organizational units related to storing UNIX data in Active Directory are created • Active Directory Groups for managing the DirectControl environment are created • Delegations are established to enable UNIX personnel to manage DirectControl in Active Directory • All final Zones are built via a set of scripts <p>A long-term UID/GID management Zone is established and all UNIX users are granted profiles in this new Zone</p>
12 - 14	<p>User and group migration.</p> <p>Key topics:</p> <ul style="list-style-type: none"> • Users and groups are migrated from local files to Active Directory; however, the local accounts are not removed, therefore allowing for a rollback strategy. • UNIX computers are joined to Active Directory during established change windows (if required) and rebooted as required • Daily status reports keep customer management aware of project progress and status
15	<p>Role-specific training.</p> <p>Key topics:</p> <ul style="list-style-type: none"> • Role-specific training is provided for UNIX user provisioning personnel • The remaining UNIX machines are joined to Active Directory and users and groups are migrated • Final status report to management

Key Assumptions

- Client understands that Centrifys performance of the Services and delivery of agreed upon deliverables under this Jump Start is dependent in part upon Client's actions, and Client therefore agrees to cooperate with Centrifys in a commercially reasonable manner in the completion of the Services by Centrifys. Centrifys will promptly notify Client of any delays of potential delays in Centrifys ability to undertake and complete performance in accordance with the applicable schedule resulting from the inaction of Client.
- Client understands that the implementation of Centrifys best practices are part of engagement estimation. It is expected that the single OU and sub-OU architecture will be implemented using our supported CreateOU powershell script, or the same architecture will be built manually before this engagement commences.
- Client will verify that each student computer for use during onsite training meets the minimum system requirements by using the system check at: <https://use.cloudshare.com/Ent/Machine.mvc/testpage>
- Client will provide the assigned consultant for the engagement a list of students for the onsite training. This list must be emailed a minimum of two weeks in advance of the scheduled training dates.
- Client will provide all hardware, software, facilities, equipment, and Client personnel (including technical resources) necessary to complete the project. These resources will be provided when they are needed in order to avoid project delays.
- Client will appoint a single point of contact for the duration of the project. This person will have project management responsibilities, be technically astute and familiar with Client change request processes as well as have the authority to expedite if necessary.
- Client management will make decisions and resolve issues in a timely manner in order to avoid project delays.
- If any Consulting Services engagement is canceled by Client less than three (3) weeks before the scheduled start date for such Services, Centrifys will most likely not be able to reschedule the engagement and be out the revenue. Centrifys will make every effort to redeploy the consultant and if Centrifys is able then the Client agrees to pay Client agrees to pay any reasonable fees and expenses incurred by Centrifys in terms of travel cancellations. If Centrifys is not able to redeploy the consultant then Client agrees to pay the full amount of the Consulting Fees that would have been properly invoiced by Centrifys had Client not canceled such engagement, and also any reasonable fees and expenses incurred by Centrifys in terms of travel cancellations. For multiple week engagements this only applies for each week that is less than the three (3) week cancellation notice.
- Client will have network connectivity and name resolution between all Client systems (including workstations and servers the Centrifys Suite will be installed on, regardless of on-premise vs. off-premise computer locations) and Active Directory connectivity functioning correctly prior to work beginning.
- Centrifys assumes that Client has a single Active Directory Forest in scope of this engagement.
- Centrifys assumes that no computers in a DMZ at Client are in the scope of this professional services engagement.
- Centrifys assumes that Client has a single logical project team in the same physical location, with representatives from the UNIX and Windows platforms participating as needed in the design discussions.
- All Client servers will be in the same data center or, if multiple data centers, there will be at least T1 connection speed between the main data center and the remote sites. It is also

recommended that resources from other sites be identified in advance as project resources, if multiple remote sites are in scope.

- Client will provide Centrifly with an associate that has the proper administrative access to all agent servers and will have the ability to reboot servers as necessary within twenty-four (24) hours of request. Any applications the customer has running on these systems that need to authenticate to the operating system could be affected after the agent is installed since Centrifly is adding Centrifly's PAM module. Some applications need to be restarted after Centrifly's agent is installed in order to run properly. There is no way Centrifly can know every application running on all of the servers of Client and how they will react. What Centrifly has found is rebooting the server is the most reliable and safest way to ensure those applications are restarted appropriately.
- Client will ensure all systems meet the minimum patch requirements and system requirements for the Centrifly Suite (see Centrifly Product Release Notes for specific platform requirements). Centrifly recommends the use of 'adcheck' to verify system requirements.
- All systems and applications that will have Centrifly's Suite of technologies installed must be on the Supported Platforms list at: <http://www.centrifly.com/directcontrol/platforms.asp>
- If the scope of this project involves any specialized customization or software development that is outside the current functionality of the Centrifly Suite of Products, that development work is subject to a 30-day warranty beginning on the completion of that development work.
- For onsite engagements five (5) business days or longer, Centrifly reserves the right to either work four ten (10) hour days or four (4) days on site and one day off site.
- All materials and information generated or used by Centrifly in the performance of the Services, including but not limited to the work product delivered to Client ("Consulting Materials"), and all intellectual property rights therein, shall be the property of Centrifly. Centrifly hereby grants to Client a personal, non-transferable, non-sublicensable, non-exclusive license to use, reproduce, copy and display any Consulting Materials solely for Company's internal business purposes. Client obtains no title or ownership in any Consulting Materials, and Centrifly retains all right, title and interest in and to any Consulting Materials. Client retains all right, title, and interest in and to Client data.
- **Engagement Management** includes activities performed in support of this Jump Start that require management expertise, oversight, control, and direction in team building, communications, time management, quality assurance and quality control and management, and cost management. Centrifly Professional Services will regularly communicate personnel and resource requirements for this Jump Start to be a success, ensure appropriate staffing and scheduling of Centrifly personnel for this Jump Start, and ensure deliverable quality and timeliness.
- **Impracticability.** Centrifly shall not be required to provide any portion of the Services to the extent the performance of such Services becomes "Impracticable" as a result of a cause or causes outside the reasonable control of Centrifly including unfeasible technological requirements, or to the extent the performance of such Services would require Centrifly to violate any applicable laws, rules or regulations or would result in the breach of any software license or other applicable contract.

Scope Change Control

- During the performance of the engagement, certain issues may arise that effectively prevent the completion of the work outlined in this Jump Start within the planned timeframe, such as, but not limited to, hardware or network failures or outages in Client's environment, problems with Client's in-house software or Client's third-party software, or the unavailability of key Client personnel. If this situation occurs, the designated Centrifly representative will work with Client to identify and document the scope change, its impact on the project approach, timing, fees, resources, and the quality of project results. Centrifly will document this using either the Centrifly Change Request Form or an appropriate Change Control form provided by Client.
- Any change in scope must be agreed to in writing prior to Centrifly reengaging on the project and will require the signature of the Centrifly Technical Services Vice President and the appropriate Client representative. Any other problems, disputes or issues arising during this engagement should be communicated as soon as possible after identification to the designated Centrifly Consultant for resolution.

Timeframe and Resources

Centrifly estimates that Centrifly's work on the project will require the number of person-days reflected in the total days below in order to complete based upon the scope and assumptions described in this Jump Start and will be performed according to the following planned schedule:

Activity	Estimated Days
Centrifly Zero Trust Privilege Services Standard Jump Start	15
Total Days	15

This proposal is based on a standard eight (8) hour workday. Any work performed in excess of a standard eight-hour workday may be subject to an hourly over time charge based on the hourly rate currently being charged to Client. If this condition occurs, Centrifly will notify the Client contact, provide a change request form and obtain approval in writing from the customer prior to the overtime work being performed.

In performing this engagement, Centrifly will assist in prioritizing and sizing Centrifly's recommended changes, and will assist with implementing the recommended changes as time permits (i.e., up to the amount of time presented in the table above). Centrifly cannot commit to assisting with implementing all of the changes Centrifly will recommend as it is impossible at this point in time to determine the amount of effort that will be required to fully implement those recommendations.

Circumstances may necessitate changes to the tasks and/or time estimates. If this situation occurs, Centrifly will follow the change control procedures in the Jump Start.

Period of Performance

The period of performance for this Jump Start begins upon the date of mutual signature by authorized representatives of Centrifly and Client and continues through the Completion Date (as defined below). All work must be scheduled to be completed within six months (180 days) of the start of the performance period. Any modifications or extensions will be requested through Change Control for review and discussion.

Completion date. The "Completion Date" will be the earlier of (1) the date on which all Services and Deliverables are completed, or (2) six months after the date of mutual signature of this Jump Start by authorized representatives of Centrify and Client.

Professional Fees and Expenses

This is a fixed price engagement. The Services will be considered completed when the deliverables are completed or when the fifteen (15) services and training days have been delivered, whichever happens first.

Personnel

Personnel Quality. Centrify agrees that all personnel used by Centrify to perform the Services will be competent and adequately trained by Centrify to perform the Services in accordance with the provisions of this Jump Start.

Background Checks. Centrify shall perform commercially reasonable background checks on all personnel assigned by Centrify to provide the Services under this Jump Start. These background checks include and are not limited to: criminal history for the past seven years, verification of employment, credit history, and education verification. Client may request in writing a letter of proof from Centrify's background check provider that the Background Check was completed successfully.

Subcontractors Permitted. Centrify may engage a Subcontractor to perform all or any portion of its duties under this Agreement provided that any such Subcontractor agrees in writing to be bound by confidentiality obligations at least as protective as the terms of this Jump Start regarding confidentiality. Subcontractors are subject to Centrify's standard Background Checks. Centrify remains responsible for the performance of such Subcontractor.

Centrify will obtain written permission from Client before assigning a Subcontractor to work on this Jump Start.

Subcontractor Defined. As used in this Agreement, "Subcontractor" will mean any individual, partnership, corporation, firm, association, unincorporated organization, joint venture, trust or other entity engaged to perform hereunder. Subcontractors will be Centrify Certified Administrators who have undergone a rigorous training program from Centrify.

Tasks to be completed by Client before Professional Services personnel arrive onsite

- Client will complete a pre-design questionnaire and return the questionnaire to their assigned consultant from Centrify Professional Services at least one week in advance of the engagement.
- Registered students will complete the online training before the onsite portion of this engagement.
- Client will determine the owner and/or responsible individual for determining privileged access to each in-scope system.
- Client will install and utilize the Centrify DirectControl agent to complete the following steps in the in-scope Active Directory Forest:
 - Step (1) Discovery of all in-scope systems; and,
 - Step (2) Download all Centrify agent software; and,
 - Step (3) Perform an adcheck analysis of all in-scope systems, and clearing any errors from the analysis that would prevent the Centrify Suite installation.
- Client will be responsible for preparing and filing change management in advance as required to prevent schedule delays
- Client will provide an inventory of all UNIX/Linux hosts to be transitioned to Active Directory.
- Client will provide an inventory of all Windows hosts expected to be part of this engagement.
- Client will provide an inventory of UNIX/Linux user identities and UNIX/Linux groups to be transitioned to Active Directory.
- Client will provide a list of identities including user accounts, generic accounts, non-system accounts that are NOT going to be migrated to DirectControl.
- Client will provide a network diagram or documentation that represents UNIX systems and the Active Directory Sites and Services.
- Client will provide availability and contact information of an Active Directory Administrator with Enterprise Forest Admin privileges.

CCS-IS-STD-JS-300

Our mission is to stop the leading cause of breaches – privileged access abuse. Centrify empowers our customers with a cloud-ready Zero Trust Privilege approach to secure access to infrastructure, DevOps, cloud, containers, Big Data and other modern enterprise attack surfaces. To learn more, visit www.centrixy.com.

Centrify is a registered trademark of Centrify Corporation. Other trademarks mentioned herein are the property of their respective owners.

©2019 Centrify Corporation. All Rights Reserved.

US Headquarters +1 (669) 444 5200
 EMEA +44 (0) 1344 317950
 Asia Pacific +61 1300 795 789
 Brazil +55 11 3958 4876
 Latin America +1 305 900 5354
sales@centrixy.com



www.centrixy.com

Centrify Connectors and Unix Servers Requirements:

Protocol	Port	Operations
API Proxy (HTTP Proxy)	8080	Type: (TCP) Source: Unix Servers Destination: Centrify Connectors Direction: Bi-Directional

IWA	8443	Type: (TCP) Source: Unix Servers Destination: Centrify Connectors Direction: Bi-Directional
-----	------	--

HTTPS	443	Type: (TCP) Source: Unix Servers Destination: Centrify Connectors Direction: Bi-Directional
-------	-----	--

Centrify Connector and Internet Connectivity:

Protocol	Port	Operations
Connector	443	Type:HTTPS (TCP) Source: Connectors Destination: outbound traffic to Internet

Service Bus	3001	Type: Customer Managed Only (TCP) Source: Connectors Destination: Internet Direction: Bi-Directional
-------------	------	---

Centrify requires the following ports for the Connector service and Domain Controllers:

Protocol	Port	Operations
DNS	53	Type: DNS (TCP,UDP) Source: Connectors Destination: Domain Controllers Direction – Bi-Directional

Global Catalog	3268	Type: Global Catalog (TCP) Direction: Connectors --> Domain Controllers
----------------	------	--

LDAP	389	Type: LDAP (TCP,UDP) Direction: Connectors --> Domain Controllers
------	-----	--

Kerberos	88	Type: Kerberos (TCP) Direction: Connectors --> Domain Controllers
----------	----	--

Kerberos Password	464	Type: Kerberos Password (TCP) Direction: Connectors --> Domain Controllers
-------------------	-----	---

SMB/CIFS	445	Type: SMB/CIFS (TCP) Direction: Connectors --> Domain Controllers
----------	-----	--

Time Service	123	Type: NTP (TCP) Direction: Connectors --> Domain Controllers
--------------	-----	---

RPC Endpoint Mapper	135	Type: RPC Mapper (TCP) Direction: Connectors --> Domain Controllers
---------------------	-----	--

RPC Endpoint (TCP Dynamic)	49153 to 65535	Type: RPC Endpoint (TCP) Direction: Connectors --> Domain Controllers
----------------------------	----------------	--

Appendix B – Firewall Rules (continued)

Centrify Privilege Service requires the following ports for the Connector service and Unix resources:

Protocol	Port	Operations
SSH	22	Type: (TCP) Source: Unix Servers Destination: Centrify Connectors Direction: Bi-Directional
HTTPS	443	Type: (TCP) Source: Unix Servers Destination: Centrify Connectors Direction: Bi-Directional
API Proxy (HTTP Proxy)	8080	Type: (TCP) Source: Unix Servers Destination: Centrify Connectors Direction: Bi-Directional
IWA	8443	CPS MFA (TCP) Direction - Unix Server to Connectors

Centrify Privilege Service requires the following ports for the Connector service and CPS portal Users:

Protocol	Port	Operations
SSH	22	Type: SSH (TCP) Direction: Workstations/Laptops --> Connectors
RDP	5555	Type: RDP (TCP) Direction: Workstations/Laptops --> Connectors

Centrify Reporting Services requires the following ports for MS SQL Server Reporting Service:

Protocol	Port	Operations
HTTP	80	HTTP SSRS URL (TCP) Direction – Centrify Management Server to MSSRS Server
HTTPS	443	HTTPS (TCP) Direction – Centrify Management Server to MSSRS Server
SQL	1433	Centrify Reporting Service (TCP) Direction – Centrify Management Server to MSSRS Server
HTTP	80	Centrify Reporting URL (TCP) Direction – User Workstation/Laptops to MSSRS Server (Optional)
HTTPS	443	Centrify Reporting URL (TCP) Direction – User Workstation/Laptops to MSSRS Server (Optional)

Centrify Reporting Services requires the following ports for the Centrify Management Server and MS SQL Server:

Protocol	Port	Operations
RPC	139	RPC (TCP) Direction - Centrify Management Server to MS SQL Server
RPC	445	RPC (TCP) Direction - Centrify Management Server to MS SQL Server
RPC	137	RPC (UDP) Direction - Centrify Management Server to MS SQL Server
RPC	138	RPC (UDP) Direction - Centrify Management Server to MS SQL Server

Appendix B – Firewall Rules (continued)

Direct Control requires the following ports for UNIX Servers and Domain Controllers:

Protocol	Port	Operations
LDAP	389	Lightweight Directory Access Protocol (TCP/UDP) Source: UNIX Servers Destination: Domain Controllers Direction: One-Way
LDAP	3268	Global Catalog Searches (TCP) Source: UNIX Servers Destination: Domain Controllers Direction: One-Way
Kerberos	88	Kerberos Authentication (TCP/UDP) Source: UNIX Servers Destination: Domain Controllers Direction: One-Way
Kerberos	464	Kerberos Password Changes (TCP/UDP) Source: UNIX Servers Destination: Domain Controllers Direction: One-Way
DNS	53	Domain Name Service lookups (TCP/UDP) Source: UNIX Servers Destination: Domain Controllers Direction: One-Way
SMB	445	Samba (TCP/UDP) Source: UNIX Servers Destination: Domain Controllers Direction: One-Way
SNTP	123	Simple Network Time Protocol (UDP) Source: UNIX Servers Destination: Domain Controllers Direction: One-Way