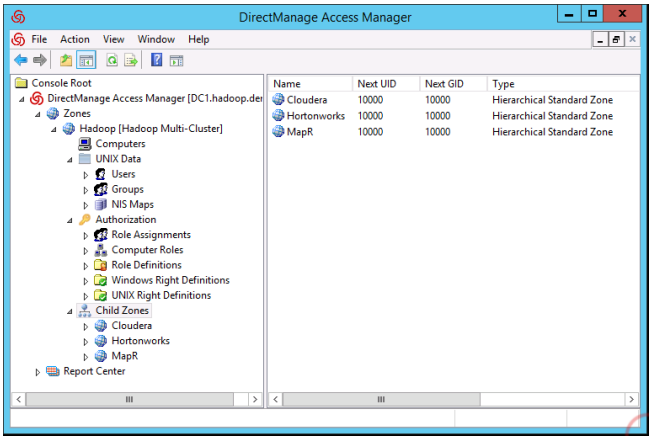
What's New in Centrify Server Suite 2015

Centrify Server Suite Standard Edition

Hadoop support



Big Data adoption by industry is around 25% on average and growing to 50% over the next 2 years, so it comes as no surprise that enterprises have been piloting and planning enterprise deployments of Hadoop. Hadoop is typically used to analyze larger volumes of data that comes from several different sources—this allows organizations to increase their data analytics capabilities.

Hadoop requires a huge number of servers in order to distribute and process massive volumes of data-—the sheer data volume is doubling every 18-24 months! As enterprises deploy these Hadoop servers (consisting of clusters with thousands of nodes), they must deal with the same challenges they have faced in deploying any server infrastructure. And enterprise IT is well aware of the challenges that large server deployments create when it comes to security, compliance, and identity related risks. Hadoop deployments often process sensitive data that may include PII, PCI, or patient data, and a Hadoop deployment may introduce identity silos that further increase risk and identity management costs.

The challenges with Hadoop are the same as those challenges that any large server deployment faces:

- High-value data = high-risk target
- Identity silos = increased risk - Organizations typically have multiple Hadoop clusters for Dev, Test, Production as well as multiple production environments for various lines of business. By consolidating identities and leveraging proven security investments, organizations can reduce cost of infrastructure and training, and reduce operational risks.
- Risk of failed audits – IT staff need access and privileges to manage clusters, and end users need to be able to submit jobs across the cluster.

The Centrify Server Suite addresses these challenges, and with the release of Centrify Server Suite 2015, customers get specific automation tools that enable rapid deployment of Hadoop in secure mode and integration with Active Directory.

Deploying Hadoop in secure mode requires Kerberos service principal management across each cluster as well as within each node. Centrify Server Suite 2015 facilitates the deployment of Hadoop in secure mode by automating the creation of Hadoop headless accounts and per node service accounts as well as providing support for Kerberos keytab management. In this way, customers are able to fully integrate their Hadoop deployments with the rest of their enterprise identity system—they can leverage an existing investment in Active Directory to provide centralized identity management and auditing across Hadoop clusters, nodes and services and seamlessly integrate identity and access management, privilege management and session monitoring across the broadest range of platforms in the industry.

This results in a more secure Hadoop environment and addresses regulatory requirements while leveraging existing infrastructure and skillsets.

Centrify Server Suite 2015 includes the following features to enable Hadoop enterprise deployment in secure mode:

- The adkeytab utility is enhanced to support computer account creation and enable long-lived accounts that must be shared across a cluster.
- A sample script is provided to automate Hadoop service account creation and keytab management. This makes deployment easier and reduces risk of error.
- Centrify Server Suite continues to support Active Directory user Kerberos credential renewal—this is called out to emphasize the importance of enterprise grade features required for continuous, secure operations.

Audit Trail Enables SIEM Integration

Security information and event management (SIEM) integrations with Server Suite are now easier, because all audit trail events are now fully documented for customer use. This enables integration with any further downstream processing of audit data—whether it be a customer-developed application or a SIEM application. Centrify Server Suite 2015 writes a unique event ID also known as Centrify Event ID for each of the Audit Trail events. On Windows clients, the audit trail event is written in Windows Application Event Logs with a unique event ID. On UNIX/Linux clients, the newly redesigned event IDs are written to syslog.

Multi-factor authentication for RedHat and Windows

- Smart card support for Red Hat Enterprise Linux 7 is available in Centrify Server Suite 2015.
- Windows support has been extended with the ability to require re-authentication with a smart card when executing a privileged command. In order to mitigate attacks such as “pass the hash”, Centrify Server Suite policy may be set to require re-authentication—this may involve re-authentication using a password or using a smart card.

Manageability Enhancements

- Configuration parameters have been updated to support a number of new parameters to enhance manageability and automation, resolve integration and deployment issues, and provide greater control for the Centrify administrator.
- Centrify Server Suite 2015 introduces new or enhanced scripts and command line utilities that provide more detailed information regarding locally effective group policy, automount map entries, non-zone users and groups, and start/stop of the Centrify LDAP Proxy.
- Access Manager now has a new wizard, "Generate Centrify Recommended Deployment Structure" to help users generate a deployment structure that follows Centrify recommended best practice.
- Centrify Server Suite 2015 delivers new Group Policies, simplifies management with the Zone Provisioning Agent, and enhances the extensions for ADUC and Group Policy Management Editor.

Other features and enhancements

- Centrify OpenSSH enhancements support SMF (Service Management Facility) on Solaris, merge parameters when upgrading stock sshd to Centrify sshd, support for alternate SPN for SSO login with GSS-API and alternate startup options.
- Centrify Server Suite 2015 updates a number of infrastructure components: OpenSSH 6.6p1, OpenSSL 0.9.8zc, curl library 7.39, dazo (based on updates in sudo-1.8.10p3), OpenLDAP 2.4.40.

Additional Supported Platforms

Support has been added for the following operating systems:

- CentOS 5.11, 6.6 (x86, x86_64)
- Debian Linux 7.7 (x86, x86_64)
- Fedora 21 (x86, x86_64)
- Linux Mint 17.1 (x86, x86_64)
- OpenSUSE 13.1, 13.2 (x86, x86_64)
- Oracle Linux 5.11, 6.6 (x86, x86_64)
- Oracle Linux 7.0 (x86_64)
- Oracle Solaris 11.2 (x86_64, Sparc 64-bit)
- Red Hat Enterprise Linux Server 5.11, 6.6 (x86, x86_64)
- Red Hat Enterprise Linux Desktop 5.11, 6.6 (x86, x86_64)
- Red Hat Enterprise Linux Server 5.10, 5.11, 7.0 (ppc64)
- Red Hat Enterprise Linux Server 5.10, 5.11 (IA64)
- Scientific Linux 5.11, 6.6 (x86, x86_64)
- Scientific Linux 7.0 (x86_64)
- Ubuntu Desktop 14.10 (x86, x86_64)
- Ubuntu Server 14.10 (x86, x86_64)
- SUSE Enterprise Linux 12 (x86_64)

Centrify Server Suite Enterprise Edition

Audit Trail Enables SIEM Integration

SIEM integrations with Server Suite are now easier, because all audit trail events are now fully documented for customer use. This enables integration with any further downstream processing of audit data—whether it be a customer-developed application or a SIEM application. Centrify Server Suite 2015 writes a unique event ID also known as Centrify Event ID for each of the Audit Trail events. On Windows clients, the audit trail event is written in Windows Application Event Logs with a unique event ID. On UNIX/Linux clients, the newly redesigned event IDs are written to syslog.

For command level auditing, an audit trail event is generated when an audited command is executed. This allows you to use SIEM monitoring tools to trigger review of the associated audit sessions. The collector from previous releases will not save this audit trail event to Audit Store database.

Performance and Operations

SQL Server connection pool tuning enables more performant and efficient audit processing

- The default maximum SQL Server connection pool size has been increased from the previous value of 300 to 1000 for the collector. The new setting allows the audit collector to serve more concurrent agents at a time without exhausting the connection pool.
- Also, the Collector Configuration Wizard, has been enhanced to configure the maximum SQL connection pool size. The configured value is displayed in the Diagnostics output in the Collector Control Panel.

The Server Suite, Enterprise Edition Agent is now more manageable and performant

- A universal script is available to control the start and stop of the Agent.
- The Agent uptime is now handled by a watchdog process that ensures the agent is running and removes the previous requirement to run as a setuid program.
- Performance enhancements for moving audit data from the Agent to the audit collector.

Controlling Audited Data and Auditing Restrictions

Assure privacy with obfuscation of sensitive data and filtering of command output

- In order to allow an organization to filter out large or potentially private information (e.g. personally identifiable information), the Centrify Server Suite 2015 adds a new group policy to control the collector behavior. Commands are detected, checked (using exact match) against the command list specified by group policy and if there is a match the command's output is never saved to the audit database.
- Some sensitive output data in an audited session on a system may not be suitable to be viewed by an auditor. Server Suite, Enterprise Edition allows the administrator to specify patterns of such data to be masked. If a pattern is matched, the data is represented in the Session Player as an asterisk (*), and the data is not searchable.

Protect stored audit sessions from viewing or tampering

- In Server Suite 2015, the audit administrator can enable policies that prevent users from reviewing or deleting their own sessions. Preventing users from reviewing their own sessions also means they cannot update the review status or comment on their sessions regardless of the rights granted by their audit role. Similarly, you can establish a policy to prevent users from deleting their own sessions regardless of the rights granted by their audit role. Both new policies are disabled by default.

Querying and Display

Session query enhancements make it easier for auditors to pinpoint audited sessions

- Audit Analyzer and the PowerShell module allow querying sessions by Session ID (GUID string format) and client Name. You can also specify the Session ID and client name as part of the AQL query in FindSessions.exe.

Management and Configuration

- With Centrify Server Suite 2015 it is easier to automate administrative audit operations using PowerShell scripts. The Centrify Audit Module for PowerShell includes cmdlets that enable the following for auditors and administrators:
    - Auditors can write PowerShell scripts to generate custom text-based reports.
    - Database administrators can write scripts to automate periodic database rotation.
    - Administrators can write PowerShell scripts to check the status of collectors or audited computers as a scheduled task, then send out an alert email if a collector or audited machine is offline.
    - Auditors can write scripts to export session transcripts for each of the sessions on a particular machine during a period of time.
    - Database administrators can a write scripts to delete audit sessions from decommissioned machines.
- The centrifyda.conf has a number of new parameters. These parameters control masking of audit data, user shell assignment, audit level override and local spool disk space warning.
- Active Directory security group(s) can be used as filtering criteria (e.g. session, AuditEvent, Report) in queries and can be specified as part of audit role definition. This audit role definition can be assigned to other users/groups, so that the users of this audit role can only see the sessions/AuditEvents/Reports generated for users of the AD security group(s).

Additional Supported Platforms

The Centrify UNIX Agent adds support for the following operating systems:

- CentOS 5.11, 6.6 (x86, x86_64)
- Debian Linux 7.7 (x86, x86_64)
- Fedora 21 (x86, x86_64)
- Linux Mint 17.1 (x86, x86_64)
- OpenSUSE 13.1, 13.2 (x86, x86_64)
- Oracle Linux 5.11, 6.6 (x86, x86_64)
- Oracle Linux 7.0 (x86_64)
- Oracle Solaris 11.2 (x86_64, Sparc 64-bit)
- Red Hat Enterprise Linux Server 5.11, 6.6 (x86, x86_64)
- Red Hat Enterprise Linux Desktop 5.11, 6.6 (x86, x86_64)
- Scientific Linux 5.11, 6.6 (x86, x86_64)
- Scientific Linux 7.0 (x86_64)
- Ubuntu Desktop 14.10 (x86, x86_64)
- Ubuntu Server 14.10 (x86, x86_64)
- SUSE Enterprise Linux 12 (x86_64)

Contact Centrify

Centrify provides unified identity management across data center, cloud and mobile environments that result in single sign-on (SSO) for users and a simplified identity infrastructure for IT. Centrify's unified identity management software and cloud-based Identity-as-a-Service (IDaaS) solutions leverage an organization's existing identity infrastructure to enable single sign-on, multi-factor authentication, privileged identity management, auditing for compliance and enterprise mobility management.

SANTA CLARA, CALIFORNIA:	+1 (669) 444-5200	EMAIL:	sales@centrify.com
EMEA:	+44 (0) 1344 317950	WEB:	http://www.centrify.com
ASIA PACIFIC:	+61 1300 795 789		
BRAZIL:	+55 11 3958 4876		
LATIN AMERICA:	+1 305 900 5354		