Microsoft Active Directory Security Assessment

This assessment offers a brief, no-cost and no-obligation expert consultation to help you significantly improve your Active Directory security posture.

HOW DOES THE SECURITY ASSESSMENT WORK?

Security and system administrators have a broad range of responsibilities, including achieving and maintaining IT security and compliance across their Microsoft environments. But, as organizations grow and expand, they often lack visibility into users, groups, permissions, applications and more which can result in compromised security and potential data loss. Knowing who can access what information in your Microsoft environment is imperative for keeping your data and users secure.

Our Microsoft Active Directory (AD) Security Assessment provides critical insight into the security of your AD environment. An experienced solutions architect will consult with your team to review your environment and help you identify opportunities for improvement. After an analysis of the configuration and operational use of your AD infrastructure, we will provide recommendations and best practices to help you get the most from your investment. At no point during the engagement will any changes be made to the environment. And you are under no obligation to purchase software, services or support.

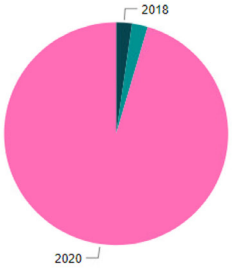
Make sure users are required to change passwords according to company policy and disable or remove unnecessary user accounts.

Service Accounts

Account Name	Password Last Changed	Password Age (Days)
svcIntrust	Tuesday, August 23, 2011	3108
svcSharepoint	Tuesday, March 20, 2012	2898
svcGPOA	Thursday, April 12, 2012	2875
svcQPM	Wednesday, September 4, 2013	2365
svcARS	Sunday, October 20, 2013	2319
svcSLAD	Wednesday, January 22, 2014	2225
svcRMAD	Monday, November 10, 2014	1933
svcSW	Monday, January 5, 2015	1877
svcMsgStats	Thursday, February 8, 2018	747
svcGlobal	Wednesday, March 28, 2018	699
svc-QCS	Thursday, March 7, 2019	355
svcAA	Wednesday, June 19, 2019	251
svcSOM	Friday, November 15, 2019	102
svcER	Saturday, November 23, 2019	94

Computer Name	Account Name
AADMIN.TITANCORP.LOCAL	TITANCORP\svcAA
APP1.TITANCORP.LOCAL	TITANCORP\svcIntrust
APP1.TITANCORP.LOCAL	TITANCORP\svcMsgStats
APP1.TITANCORP.LOCAL	TITANCORP\svcQPM
APP2.TITANCORP.LOCAL	TITANCORP\svcER
APP2.TITANCORP.LOCAL	TITANCORP\svcGPOA
APP2.TITANCORP.LOCAL	TITANCORP\svcSLAD
APP2.TITANCORP.LOCAL	TITANCORP\svcSW
APP3.TITANCORP.LOCAL	TITANCORP\svcARS
APP3.TITANCORP.LOCAL	TITANCORP\svcER
APP4.TITANCORP.LOCAL	TITANCORP\svcIntrust
APP4.TITANCORP.LOCAL	TITANCORP\svc-QCS
APP5.TITANCORP.LOCAL	TITANCORP\svcER
APP5.TITANCORP.LOCAL	TITANCORP\svcGPOA
AZADCON.TITANCORP.LOCAL	TITANCORP\svcER
AZADGATE.TITANCORP.LOCAL	TITANCORP\svcER
ITSEARCH.TITANCORP.LOCAL	TITANCORP\svcIntrust

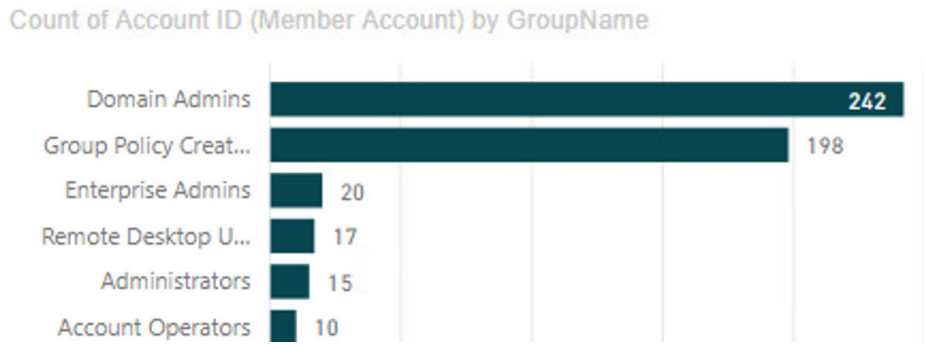
Last Logon Date



Account Name	Service Display Name
TITANCORP\svcAA	Active Administrator Agent
TITANCORP\svcAA	Active Administrator Data Services
TITANCORP\svcAA	Active Administrator Directory Analyzer Agent
TITANCORP\svcAA	Active Administrator Notification Service
TITANCORP\svcARS	Active Roles Administration Service
TITANCORP\svcARS	Active Roles Synchronization Service
TITANCORP\svcER	Quest Access Explorer Agent for TITANCORP\NETAPP Servi
TITANCORP\svcER	Quest Enterprise Reporter Node
TITANCORP\svcER	Quest Enterprise Reporter Server
TITANCORP\svcGlobal	Quest InTrust Agent
TITANCORP\svcGPOA	GPOADmin Dashboard Service Host
TITANCORP\svcGPOA	GPOADmin Service
TITANCORP\svcGPOA	GPOADmin Watcher Service
TITANCORP\svcIntrust	Quest InTrust Real-Time Monitoring Server
TITANCORP\svcIntrust	Quest InTrust Server
TITANCORP\svcIntrust	Quest IT Security Search Warehouse API

Service accounts should have specific use identified. To ensure this account is not misused you may consider setting up an alert to notify you when the account has activity originating from an unintended source.

Group analysis recommendations include understanding VIP group members, reviewing access and recognizing changes to group membership.



Review group membership as well as how groups are being used. If a group is no longer needed, it should be retired.

INITIAL ASSESSMENT

Data collection is the key component of a successful engagement. Designed to take advantage of native Windows protocols, Enterprise Reporter is designed to have no impact on your ongoing business so you can better understand who has access to what.

The following items are required to enable an effective assessment:

- High-end workstation or server-class machine
  - Windows 7 SP 1 or greater
  - Windows Server 2008 SP 2 or greater
- Domain Functional Level 2003 or greater
- Microsoft SQL Server 2008 SP 2 or greater
- PowerShell 3.0
- Microsoft .NET Framework 4.6
- Permissions for collections:
  - An account with AD read permissions

AREAS OF FOCUS

The architects will provide analysis of a comprehensive set of data relating to Active Directory including:

- Domain Groups and Members
- Domain Users
- Domain Summary
- Active Directory Permissions
- Group Policy Permissions

CONTINUOUS ASSESSMENT

Quest has the goal to ensure ongoing security needs of your organization are met. As part of this goal, our architects will enable your staff to continue utilizing Enterprise Reporter. It will remain available for use within your organization for up to six months following the engagement.

ABOUT QUEST

Quest provides software solutions for the rapidly changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid data centers, security threats and regulatory requirements. Our portfolio includes solutions for database management, data protection, unified endpoint management, identity and access management and Microsoft platform management.

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

Datasheet-AD-Security-US-TJ-58890